IMPLEMENTIERUNGSLEITFADEN

EMC VSPEX-ANWENDER-COMPUTING Citrix XenDesktop 7.5 und VMware vSphere mit EMC XtremIO

Unterstützt durch EMC VNX und EMC Datensicherheit

EMC VSPEX

Zusammenfassung

In diesem Implementierungsleitfaden werden die allgemeinen Schritte zur Bereitstellung einer EMC® VSPEX®-Lösung für Anwender-Computing für Citrix XenDesktop und VMware vSphere unterstützt durch EMC XtremIO, EMC VNX®-Speicher und EMC Datensicherheit beschrieben.

September 2014

EMC²

Copyright © 2014 EMC Deutschland GmbH. Alle Rechte vorbehalten.

Veröffentlicht im September 2014

EMC ist der Ansicht, dass die Informationen in dieser Veröffentlichung zum Zeitpunkt der Veröffentlichung korrekt sind. Diese Informationen können jederzeit ohne vorherige Ankündigung geändert werden.

Die Informationen in dieser Veröffentlichung werden ohne Gewähr zur Verfügung gestellt. Die EMC Corporation macht keine Zusicherungen und übernimmt keine Haftung jedweder Art im Hinblick auf die in diesem Dokument enthaltenen Informationen und schließt insbesondere jedwede implizite Haftung für die Handelsüblichkeit und die Eignung für einen bestimmten Zweck aus. Für die Nutzung, das Kopieren und die Verbreitung der in dieser Veröffentlichung beschriebenen Software von EMC ist eine entsprechende Softwarelizenz erforderlich.

EMC², EMC und das EMC Logo sind eingetragene Marken oder Marken der EMC Corporation in den USA und anderen Ländern. Alle anderen in diesem Dokument erwähnten Marken sind das Eigentum ihrer jeweiligen Inhaber.

Eine aktuelle Liste der Produkte von EMC finden Sie unter EMC Corporation Trademarks auf http://germany.emc.com.

EMC VSPEX Anwender-Computing
Citrix XenDesktop 7.5 und VMware vSphere mit EMC XtremIO
Unterstützt durch EMC VNX und EMC Datensicherheit
Implementierungsleitfaden

Art.-Nr. H13365

Inhalt

Kapitel 1 Einführung 9
Zweck dieses Leitfadens....10
Geschäftlicher Nutzen....10
Umfang....11
Zielgruppe....11
Terminologie....12

Kapitel 2 Bevor Sie beginnen 13
Übersicht....14
Aufgaben vor der Bereitstellung....14
Bereitstellungsworkflow....15
Grundlegende Dokumente....15
Übersicht über die Lösungen von VSPEX....15
VSPEX-Designleitfaden....15
Handbuch zur VSPEX Proven Infrastructure....16
Leitfaden: RSA SecurID für VSPEX-Anwender-Computing....16
Voraussetzungen für die Bereitstellung....16

Kapitel 3 Lösungsüberblick 19
Übersicht....20
VSPEX Proven Infrastructures....20
Lösungsarchitektur....21
Allgemeine Architektur....21
Logische Architektur....23
Übersicht über die Kernkomponenten....24

Kapitel 4 Lösungsimplementierung 27
Übersicht....28
Netzwerkimplementierung....29
Konfigurieren des Infrastrukturnetz-werks....29
Konfiguration der VLANs....31
Konfigurieren des Speichernetzwerks....31
Verkabeln des Netzwerks....32
Vorbereiten und Konfigurieren der Speicherarrays....32
Vorbereiten und Installieren von XtremIO....33
Einrichten der XtremIO-Erstkonfiguration....33
Konfigurieren von XtremIO-Ereignishandlern....33
Speicher-Provisioning für VMFS-Datastores....35

Vorbereiten der VNX....36
Einrichten der VNX-Erstkonfiguration....36
Konfigurieren von VNX Fast Cache....36
Provisioning von optionalem VNX-Speicher für Benutzerdaten....38
Konfigurieren von FAST VP für Benutzerdaten (optional)....38
Anforderungen der VSPEX Private Cloud....40
Anforderungen von Citrix ShareFile....40
Installieren und Konfigurieren der vSphere-Hosts....41
Installieren von vSphere....41
Konfigurieren des vSphere-Netzwerks....41
Verbinden von vSphere-Datastores....42
Optimieren von vSphere für XtremIO....43
Installieren und Konfigurieren der SQL Server-Datenbank....44
Bereitstellen von VMware vCenter Server....45
Installieren und Konfigurieren der XenDesktop Delivery Controller....46
Installieren der serverseitigen Komponenten von XenDesktop....47
Konfigurieren eines Standorts....48
Hinzufügen eines zweiten Controllers....48
Installieren von Citrix Studio....48
Vorbereiten der virtuellen Mastermaschine....48
Provisioning der virtuellen Desktops....49
Installieren und Konfigurieren von Citrix Provisioning Services....49
Konfigurieren einer PVS-Serverfarm....50
Hinzufügen eines zweiten PVS-Servers....50
Erstellen eines PVS-Speichers....50
Konfigurieren der eingehenden Kommunikation....51
Konfigurieren einer Bootstrap-Datei....51
Konfigurieren der Startoptionen 66 und 67 auf dem DHCP-Server....52
Vorbereiten der virtuellen Mastermaschine....52
Provisioning der virtuellen Desktops....52
Einrichten von EMC Avamar....53
Übersicht über die Avamar-Konfiguration....53
Konfigurieren von GPO-Ergänzungen (Group Policy Object) für Avamar....55
Windows-Sicherheit für den Avamar Client-Service....59
Definieren von Avamar-Datasets....60
Definieren von Avamar-Backupplänen....63
Anpassen der Wartungsfen-sterplanung....63
Definieren von Avamar-Aufbewahrungs-Policies....65
Erstellen einer Avamar-Gruppe und Gruppen-Policy....65
Aktivieren von XenDesktop-Clients (Desktops)....67

Kapitel 5 Lösungsverifizierung 75
Übersicht....76
Checkliste nach der Installation....77
Bereitstellen und Testen eines einzelnen virtuellen Desktop....77
Überprüfen der Redundanz der Lösungskomponenten....77

Kapitel 6 Referenzdokumentation 79
EMC Dokumentation....80
Andere Dokumentationen....80

Anhang A Konfigurationsarbeitsblatt 83
Arbeitsblatt für die Kundenkonfiguration....84

Abbildungen

Abbildung 1. VSPEX Proven Infrastructures 21
Abbildung 2. Architektur der validierten Lösung 22
Abbildung 3. Logische Architektur für Block- und Filespeicher 23
Abbildung 4. Beispiel-Ethernetnetzwerkarchitektur 30
Abbildung 5. Beispiel für eine Fibre-Channel-Netzwerkarchitektur 31
Abbildung 6. Schaltfläche „XtremIO Display Event Handlers“ 34
Abbildung 7. XtremIO-Fenster „Edit Event Handler“ 34
Abbildung 8. Dialogfeld Storage System Properties 36
Abbildung 9. Erstellen des FAST Cache-Dialogfelds 37
Abbildung 10. Dialogfeld Storage Pool Properties 39
Abbildung 11. Das Fenster „Manage Auto-Tiering“ 39
Abbildung 12. Dialogfeld Configure Bootstrap 51
Abbildung 13. Konfigurieren der Windows-Ordnerumleitung 55
Abbildung 14. Öffnen des Dialogfelds Mapped Drive Properties 56
Abbildung 15. Erstellen einer Windows-Netzwerklaufwerkzuordnung für Benutzerdateien 57
Abbildung 16. Konfigurieren der gemeinsamen Einstellungen für die Laufwerkszuordnung 58
Abbildung 17. Erstellen einer Windows-Netzwerklaufwerkzuordnung für Benutzerprofildaten 59
Abbildung 18. Konfigurieren der Windows-Ordnerumleitung 60
Abbildung 19. Konfigurieren der Einstellungen für das Avamar-Dataset 61
Abbildung 20. Ausschlusseinstellungen für das Benutzerprofil-Dataset 62
Abbildung 21. Option Select Plug-in Type 62
Abbildung 22. Optionen zum Sperren von Volumes 63
Abbildung 23. Standardplanung für Backup-/Wartungszeitfenster von Avamar 64
Abbildung 24. Geänderte Planung für Backup-/Wartungszeitfenster in Avamar 65
Abbildung 25. Erstellen einer neuen Avamar-Backupgruppe 66
Abbildung 26. Fenster New Group 66
Abbildung 27. Auswählen eines vorhandenen Plans 67
Abbildung 28. Avamar Enterprise Manager-Dashboard 68
Abbildung 29. Avamar Client Manager 68
Abbildung 30. Menü mit Clientinformationen 69
Abbildung 31. Dialogfeld Directory Service 69
Abbildung 32. EMC Avamar Client Manager mit Active Directory-Informationen 70
Abbildung 33. Virtuelle VSPEX-Desktops 70
Abbildung 34. Ausgewählte virtuelle Desktops 71
Abbildung 35. Fenster Select Groups 71
Abbildung 36. Aktivieren der Domain 72
Abbildung 37. Fenster Show Clients for Activation 72
Abbildung 38. Avamar Client Manager mit aktivierten Clients 73
Abbildung 39. Öffnen von Anhängen in einer PDF-Datei 84

Tabellen

Tabelle 1. Terminologie 12
Tabelle 2. Aufgaben vor der Bereitstellung 14
Tabelle 3. Bereitstellungsworkflow 15
Tabelle 4. Checkliste für die Bereitstellungsvoraussetzungen 16
Tabelle 5. Komponenten der VSPEX-Lösung 24
Tabelle 6. Überblick über den Implementierungsprozess 28
Tabelle 7. Aufgaben für die Switch- und Netzwerkkonfiguration 29
Tabelle 8. Aufgaben für die Speicherkonfiguration 32
Tabelle 9. Volumes auf der XtremIO zum Speichern virtueller Desktops 35
Tabelle 10. Erstellen eines blockbasierten RAID 6-Speicherpools 38
Tabelle 11. Konfigurieren von LUNs für NAS-Pools 38
Tabelle 12. Mindestanforderungen für den Infrastrukturserver 40
Tabelle 13. Minimum der Hardwareressourcen für ShareFile StorageZones mit Storage Center 40
Tabelle 14. Empfohlener VNX-Speicher der CIFS-Share für ShareFile StorageZones 40
Tabelle 15. Aufgaben für die Serverinstallation 41
Tabelle 16. Aufgaben für die SQL Server-Datenbankkonfiguration 44
Tabelle 17. Aufgaben für die vCenter-Konfiguration 45
Tabelle 18. Aufgaben für die Einrichtung der XenDesktop-Controller 47
Tabelle 19. Aufgaben für die Einrichtung der XenDesktop-Controller 49
Tabelle 20. Aufgaben für die Avamar-Integration 53
Tabelle 21. Aufgaben für das Testen der Installation 76
Tabelle 22. Allgemeine Serverinformationen 84
Tabelle 23. vSphere-Serverinformationen 85
Tabelle 24. XtremIO-Arrayinformationen 85
Tabelle 25. VNX-Arrayinformationen 85
Tabelle 26. Informationen zur Netzwerkinfrastruktur 85
Tabelle 27. VLAN-Informationen 86
Tabelle 28. Servicekonten 86

Kapitel 1 Einführung

In diesem Kapitel werden die folgenden Themen behandelt:

Zweck dieses Leitfadens 10

Geschäftlicher Nutzen 10

Umfang 11

Zielgruppe 11

Terminologie 12

Zweck dieses Leitfadens

Mit der EMC® VSPEX® Proven Infrastructure für Anwender-Computing erhält der Kunde ein modernes System, mit dem eine große Zahl virtueller Desktops auf einem konsistenten Performancelevel gehostet werden kann. Diese VSPEX-Lösung für Anwender-Computing für Citrix XenDesktop 7.5 wird auf einer VMware vSphere-Virtualisierungsebene ausgeführt, die von der hoch verfügbaren EMC XtremIO-Produktreihe unterstützt wird, die den Speicher bereitstellt. In dieser Lösung werden die Komponenten der Desktopvirtualisierungsinfrastruktur auf einer VSPEX Private Cloud für VMware vSphere Proven Infrastructure ausgeführt, während die Desktops auf dedizierten Ressourcen gehostet werden.

Die Rechner- und Netzwerkkomponenten, die von den VSPEX-Partnern definiert werden, sind redundant und ausreichend leistungsstark ausgelegt, um die Verarbeitungs- und Datenanforderungen einer großen virtuellen Desktopumgebung zu bewältigen. EMC XtremIO-Lösungen bieten Speicherplatz für virtuelle Desktops, EMC VNX-Lösungen bieten Speicher für Benutzerdaten, EMC Avamar®-Datensicherheitslösungen bieten Datensicherheit für Citrix XenDesktop-Daten und RSA® SecurID® bietet optionale Funktionen für eine sichere Benutzerauthentifizierung.

Diese VSPEX-Lösung für Anwender-Computing ist validiert für bis zu 1.750 Citrix XenDesktop MCS-verknüpfte Clones (Machine Creation Services) oder Citrix PVS-gestreamte virtuelle Desktops (Provisioning Services) für einen Starter X-Brick und bis zu 3.500 MCS-verknüpfte Clones oder PVS-gestreamte virtuelle Desktops für einen X-Brick. Die validierten Konfigurationen basieren auf einem Referenzdesktop-Workload und bilden die Basis für die Erstellung kostengünstiger, benutzerdefinierter Lösungen für einzelne Kunden.

Eine Infrastruktur für Anwender-Computing oder virtuelle Desktops ist ein komplexes Systemangebot. In diesem Implementierungsleitfaden wird beschrieben, wie Sie mithilfe von Best Practices die erforderlichen Ressourcen für die Bereitstellung einer Anwender-Computing-Lösung für Citrix XenDesktop für VMware vSphere, unterstützt durch EMC XtremIO, EMC VNX und EMC Datensicherheit, implementieren.

Geschäftlicher Nutzen

Mitarbeiter sind mobiler als je zuvor und sie erwarten Zugriff auf geschäftskritische Daten und Anwendungen, jederzeit und überall und von jedem beliebigen Gerät aus. Sie möchten ihre eigenen Geräte zur Arbeit mitbringen können, sodass IT-Abteilungen zunehmend BYOD-Initiativen (Bring Your Own Device) in Erwägung ziehen und unterstützen. Dadurch nimmt die Komplexität im Bezug auf den Schutz von vertraulichen Informationen zu. Die Bereitstellung virtueller Desktops bietet hier eine Möglichkeit.

Die Implementierung umfangreicher virtueller Desktopumgebungen bringt jedoch auch viele Herausforderungen mit sich. Administratoren müssen schnell sowohl persistente als auch nicht-persistente Desktops für alle Benutzer (aufgabenorientierte Mitarbeiter, normale Mitarbeiter und Hauptbenutzer) bereitstellen, ohne die einer Umgebung mit physischen Desktops überlegene hervorragende Benutzererfahrung zu mindern.

Neben der erforderlichen Performance muss eine virtuelle Desktoplösung einfach bereitzustellen, zu managen und zu skalieren sein, mit bedeutenden Kosteneinsparungen gegenüber physischen Desktops. Speicher ist ebenfalls eine wichtige Komponente einer effektiven virtuellen Desktoplösung. EMC VSPEX Proven Infrastructures sind darauf ausgerichtet, Ihnen dabei zu helfen, die schwierigsten Herausforderungen in der IT zu bewältigen, indem einfache, effiziente und flexible Lösungen bereitgestellt werden, die dazu entwickelt wurden, die zahlreichen Funktionen der XtremIO-Flashtechnologie zu nutzen.

Die VSPEX-Lösung für Anwender-Computing für Citrix XenDesktop bietet unter anderem die folgenden geschäftlichen Vorteile:

- Eine End-to-End-Virtualisierungslösung zur Nutzung der Funktionen der einheitlichen Infrastrukturkomponenten
- Effiziente Virtualisierung für verschiedene Anwendungsbeispiele mit bis zu 1.750 MCS-verknüpften Clones oder PVS-gestreamten virtuellen Desktops für einen Starter X-Brick und bis zu 3.500 MCS-verknüpften Clones oder PVS-gestreamten virtuellen Desktops für einen X-Brick
- Zuverlässige, flexible und skalierbare Referenzarchitekturen

Umfang

In diesem Implementierungsleitfaden werden die allgemeinen Schritte zur Bereitstellung der VSPEX-Lösung für Anwender-Computing für Citrix XenDesktop 7.5 beschrieben. Der Leitfaden liefert ein Bereitstellungsbeispiel eines virtuellen Desktopspeichers auf EMC XtremIO und eines Benutzerdatenspeichers auf einem VNX-Speicherarray der nächsten Generation. Die für diese Lösung erforderlichen Infrastrukturserver wurden für die Ausführung auf einer VSPEX Private Cloud mit VMware vSphere Proven Infrastructure entworfen. Dieselben Prinzipien und Richtlinien gelten auch für die XtremIO- und VNX-Arrays, die im Rahmen des VSPEX-Programms von EMC validiert wurden.

Die optionale RSA SecurID-Lösung für sichere Benutzerauthentifizierung für XenDesktop wird im separaten Dokument *Sicherung des EMC VSPEX-Anwender-Computings mit RSA SecurID: Citrix XenDesktop 7 und VMware vSphere 5.1 für bis zu 2.000 virtuelle Desktops – Designleitfaden* beschrieben.

Zielgruppe

Dieser Leitfaden richtet sich an interne Mitarbeiter von EMC und qualifizierte EMC VSPEX-Partner. In diesem Leitfaden wird davon ausgegangen, dass VSPEX-Partner, die beabsichtigen, diese VSPEX Proven Infrastructure für Citrix XenDesktop bereitzustellen, über die erforderliche Schulung und den entsprechenden Hintergrund verfügen, um eine Anwender-Computing-Lösung auf der Basis von Citrix XenDesktop mit VMware vSphere als Hypervisor, XtremIO und VNX-Speichersystemen und die damit verbundene Infrastruktur installieren und konfigurieren zu können.

Leser sollten außerdem mit den Infrastruktur- und Datenbanksicherheitsrichtlinien der Kundeninstallation vertraut sein.

In diesem Leitfaden werden gegebenenfalls externe Referenzen bereitgestellt. Partner, die diese Lösung implementieren, sollten mit diesen Dokumenten vertraut sein. Weitere Details finden Sie unter Grundlegende Dokumente und Kapitel 6: Referenzdokumentation.

Terminologie

In Tabelle 1 führt die in diesem Handbuch verwendete Terminologie auf.

Tabelle 1. Terminologie

Begriff	Definition
Datendeduplizierung	Eine Funktion des XtremIO-Arrays, das die Auslastung des physischen Speichers reduziert, indem redundante Datenblöcke eliminiert werden.
PVS-gestreamte Desktops	Desktops, die als PVS-gestreamte Desktops bereitgestellt werden und ihre Basis-Image-Daten von Citrix Provisioning Services-Servern (PVS) streamen, wobei alle Änderungen je nach Desktopkonfiguration in den lokalen Schreibcache oder auf Citrix Personal vDisk geschrieben werden.
MCS-verknüpfte Clones	Desktops, die als MCS-verknüpfte Clones bereitgestellt werden und ein gemeinsames Basis-Image innerhalb eines Desktoppools verwenden und daher nur sehr wenig Speicherplatz belegen.
Referenzarchitektur	Die validierte Architektur, die diese VSPEX-Lösung für Anwender-Computing an zwei bestimmten Punkten unterstützt, d. h. 1.750 MCS-verknüpfte Clones oder PVS-gestreamte virtuelle Desktops und 3.500 MCS-verknüpfte Clones oder PVS-gestreamte virtuelle Desktops.
Referenz-Workload	Für VSPEX-Lösungen für Anwender-Computing wird der Referenz-Workload als ein einziger virtueller Desktop (der virtuelle Referenzdesktop) definiert, der die im Designleitfaden aufgeführten Workload-Merkmale aufweist. Durch den Vergleich der tatsächlichen Auslastung des Kunden mit diesem Referenz-Workload können Sie ableiten, welche Referenzarchitektur Sie als Basis für die VSPEX-Bereitstellung des Kunden auswählen sollten. Weitere Informationen finden Sie im Designleitfaden *EMC VSPEX-ANWENDER-COMPUTING: Citrix XenDesktop 7.5 und VMware vSphere mit EMC XtremIO unterstützt durch EMC VNX und EMC Datensicherheit*.
Speicherprozessor (SP)	Die Rechnerkomponente des VNX-Speicherarrays. SPs werden für alle Aspekte der Datenverlagerung in, aus und zwischen VNX-Arrays eingesetzt.
Speicher-Controller (SC)	Die Rechnerkomponente des XtremIO-Speicherarrays. SCs werden für alle Aspekte der Datenverlagerung in, aus und zwischen XtremIO-Arrays eingesetzt.
Virtual Desktop Infrastructure (VDI)	Das Anwender-Computing entkoppelt den Desktop von der physischen Maschine. In einer VDI-Umgebung werden Desktopbetriebssystem (BS) und Anwendungen innerhalb einer virtuellen Maschine auf einem Hostcomputer ausgeführt; die Daten befinden sich auf einem gemeinsamen Speicher. Die Benutzer können von jedem Computer oder Mobilgerät aus über ein privates Netzwerk oder eine Internetverbindung auf ihren virtuellen Desktop zugreifen.
XtremIO Management Server (XMS)	Wird als virtuelle Maschine bereitgestellt und für die Verwaltung des XtremIO-Arrays verwendet. Der XMS wird mithilfe eines Open Virtualization Appliance (OVA)-Pakets bereitgestellt.

Kapitel 2 Bevor Sie beginnen

In diesem Kapitel werden die folgenden Themen behandelt:

Übersicht 14

Aufgaben vor der Bereitstellung 14

Bereitstellungsworkflow 15

Grundlegende Dokumente 15

Voraussetzungen für die Bereitstellung 16

Übersicht

In diesem Kapitel erhalten Sie einen Überblick über wichtige Informationen, die Sie kennen, Dokumente, mit denen Sie vertraut sein, und Aufgaben, die Sie ausführen müssen, bevor Sie mit der Implementierung der VSPEX-Lösung für Anwender-Computing mit Citrix XenDesktop beginnen.

Im Designleitfaden für diese Lösung: *EMC VSPEX-ANWENDER-COMPUTING: Citrix XenDesktop 7.5 und VMware vSphere mit EMC XtremIO unterstützt durch EMX VNX und EMC Datensicherheit* wird beschrieben, wie Sie Ihre Lösung entwerfen und dimensionieren, Ressourcen gemäß Best Practices zuweisen und alle Vorteile von VSPEX nutzen können. Die Beispiele für Bereitstellungen in diesem Implementierungsleitfaden beruhen auf den Empfehlungen und Beispielen des Designleitfadens.

Aufgaben vor der Bereitstellung

Zu den Aufgaben vor der Bereitstellung zählen Verfahren, die nicht direkt mit der Installation und Konfiguration der Umgebung zusammenhängen, sondern deren Ergebnisse zum Zeitpunkt der Installation benötigt werden. Zu den Aufgaben vor der Bereitstellung gehören das Erfassen von Hostnamen, IP-Adressen, IDs der virtuellen LANs, Lizenzschlüsseln, Installationsmedien und so weiter. Diese Aufgaben sollten vor dem Besuch beim Kunden erledigt werden, um den Zeitaufwand vor Ort so gering wie möglich zu halten.

Tabelle 2. Aufgaben vor der Bereitstellung

Aufgabe	Beschreibung	Referenz
Sammeln von Dokumenten	Sammeln Sie die in Grundlegende Dokumente und Referenzdokumentation aufgelisteten Dokumente. Diese werden im gesamten Dokument dafür verwendet, Details zu Einrichtungsverfahren sowie Best Practices für die Dimensionierung und Bereitstellung der verschiedenen Komponenten der Lösung zur Verfügung zu stellen.	• Grundlegende Dokumente • Referenzdo-kumentation
Sammeln von Tools	Sammeln Sie die erforderlichen und optionalen Tools für die Bereitstellung. Verwenden Sie Tabelle 4, um zu bestätigen, dass die gesamte Hardware, Software und die entsprechenden Lizenzen vor dem Bereitstellungsprozess verfügbar sind.	Checkliste für die Bereitstellungsvorausse tzungen
Sammeln von Daten	Sammeln Sie die kundenspezifischen Konfigurationsdaten für Netzwerk, Arrays, Konten usw. Geben Sie diese Daten in das Arbeitsblatt für die Kundenkonfiguration ein, das Sie während des Bereitstellungsprozesses als Referenz verwenden können. Füllen Sie zusätzlich die relevante XtremIO-Checkliste für Aufgaben vor der Installation und das VNX-Arbeitsblatt aus, um umfassende arrayspezifische Informationen zur Hand zu haben. Diese Dokumente stehen auf der EMC Online Support-Website zur Verfügung.	• *XtremIO-Speicherarray – Checkliste für Aufgaben vor der Installation* • *VNX Installation Assistant for File/Unified – Arbeitsblatt* • Arbeitsblatt für die Kundenkonfi-guration

Bereitstellungsworkflow

Ziehen Sie für das Design und die Implementierung Ihrer Anwender-Computing-Lösung den Prozessablauf in Tabelle 3 zurate.

Tabelle 3. Bereitstellungsworkflow

Schritt	Aktion
1	Verwenden Sie das Arbeitsblatt für die Kundenkonfiguration im Designleitfaden, um Kundenanforderungen zu erfassen.
2	Verwenden Sie das EMC VSPEX-Dimensionierungstool, um die empfohlene VSPEX-Referenzarchitektur für Ihre Anwender-Computing-Lösung auf Basis der in Schritt 1 erfassten Benutzeranforderungen zu ermitteln. Weitere Informationen zum Dimensionierungstool finden Sie unter EMC VSPEX Sizing Tool Portal. **Hinweis:** Sollte das Dimensionierungstool nicht zur Verfügung stehen, können Sie die Anwendung anhand der Richtlinien im Designleitfaden manuell dimensionieren.
3	Legen Sie das endgültige Design der VSPEX-Lösung mithilfe des Designleitfadens fest. **Hinweis:** Stellen Sie sicher, dass alle Ressourcenanforderungen und nicht nur die Anforderungen für das Anwender-Computing berücksichtigt werden.
4	Wählen Sie die korrekte VSPEX-Referenzarchitektur und Proven Infrastructure aus und bestellen Sie sie. Empfehlungen zur Auswahl einer Private Cloud Proven Infrastructure finden Sie im VSPEX Proven Infrastructure-Leitfaden unter Grundlegende Dokumente.
5	Befolgen Sie diesen Implementierungsleitfaden zum Bereitstellen und Testen Ihrer VSPEX-Lösung. **Hinweis**: Wenn Sie bereits über eine VSPEX Proven Infrastructure-Umgebung verfügen, können Sie die bereits abgeschlossenen Schritte für die Implementierung überspringen.

Grundlegende Dokumente

EMC empfiehlt, die folgenden Dokumente zu lesen, die Sie im Bereich „VSPEX“ im EMC Community Network, unter http://germany.emc.com oder im VSPEX Proven Infrastructure-Partnerportal finden.

Übersicht über die Lösungen von VSPEX

Weitere Informationen finden Sie im *EMC VSPEX-Lösung für Anwender-Computing – Lösungsüberblick*.

VSPEX-Designleitfaden

Weitere Informationen finden Sie im *EMC VSPEX-Anwender-Computing: Citrix XenDesktop 7.5 und VMware vSphere mit XtremIO – Designleitfaden*.

Handbuch zur VSPEX Proven Infrastructure

Weitere Informationen finden Sie im *EMC VSPEX Private Cloud: VMware vSphere 5.5 für bis zu 1.000 virtuelle Maschinen – Handbuch zur Proven Infrastructure-Lösung.*

Leitfaden: RSA SecurID für VSPEX-Anwender-Computing

Weitere Informationen finden Sie im *Sicherung des EMC VSPEX-Anwender-Computings mit RSA SecurID: Citrix XenDesktop 7 und VMware vSphere 5.1 für bis zu 2.000 virtuelle Desktops – Designleitfaden.*

Voraussetzungen für die Bereitstellung

In Tabelle 4 gibt die Hardware-, Software- und Lizenzanforderungen für die Konfiguration der Lösung an. Weitere Informationen zu diesen Anforderungen finden Sie auf der EMC Online Support-Website.

Tabelle 4. Checkliste für die Bereitstellungsvoraussetzungen

Anforderung	Beschreibung
Hardware	• Physische Server mit ausreichend Kapazität zum Hosten der virtuellen Desktops gemäß den Empfehlungen im Designleitfaden • VMware vSphere-Server zum Hosten der virtuellen Infrastrukturserver • Für das Anwender-Computing erforderliche Netzwerk-Switch-Portkapazität und -funktionen • EMC XtremIO-Array mit der erforderlichen Konfiguration • EMC VNX-Multiprotokollspeicher-Array mit dem erforderlichen Laufwerkslayout **Hinweis**: Diese Anforderungen werden möglicherweise durch eine vorhandene Infrastruktur erfüllt.
Software	Installationsmedien für VMware vSphere 5.5 Installationsmedien für VMware vCenter Server 5.5 OVA-Datei für EMC XtremIO Management Server EMC Virtual Storage Integrator (VSI) für VMware vSphere: Unified Storage Management EMC VSI für VMware vSphere Storage Viewer EMC PowerPath® Viewer EMC PowerPath Virtual Edition (PowerPath/VE) Installationsmedien für Microsoft Windows Server 2012 R2 (empfohlenes Betriebssystem für VMware vCenter, Citrix XenDesktop Delivery Controller und Citrix Provisioning-Server) Installationsmedien für Microsoft Windows 8.1 Installationsmedien für Microsoft SQL Server 2012 oder höher **Hinweis**: Diese Anforderung wird möglicherweise durch die vorhandene Infrastruktur erfüllt.

Anforderung	Beschreibung
Lizenzen	Lizenzschlüssel für VMware vSphere 5.5 (Infrastruktur-Serverhosts) Lizenzschlüssel für VMware vCenter Server 5.5 Lizenzschlüssel für VMware vSphere Desktop (virtuelle Desktophosts) Lizenzschlüssel für Microsoft Windows Server 2012 R2 Standard Edition (oder höher) **Hinweis**: Diese Anforderung wird möglicherweise durch einen vorhandenen Microsoft Key Management Server (KMS) abgedeckt. Lizenzschlüssel für Microsoft Windows 8,1 **Hinweis**: Diese Anforderung wird möglicherweise durch einen vorhandenen Microsoft Key Management Server (KMS) abgedeckt. Lizenzschlüssel für Microsoft SQL Server 2012 **Hinweis**: Diese Anforderung wird möglicherweise durch eine vorhandene Lizenz abgedeckt.
Lizenzen	Lizenzdateien für EMC PowerPath Virtual Edition

Kapitel 3 Lösungsüberblick

In diesem Kapitel werden die folgenden Themen behandelt:

Übersicht 20

VSPEX Proven Infrastructures 20

Lösungsarchitektur 21

Übersicht über die Kernkomponenten 24

Übersicht

In diesem Kapitel finden Sie einen Überblick über die VSPEX-Lösung für Anwender-Computing für Citrix XenDesktop auf VMware vSphere und die wichtigsten in der Lösung verwendeten Technologien. Die Lösung wurde von EMC entwickelt und erprobt und bietet die für die Unterstützung von Referenzarchitekturen mit bis zu 1.750 MCS-verknüpften Clones oder PVS-gestreamten virtuellen Desktops für einen Starter X-Brick und bis zu 3.500 MCS-verknüpften Clones oder PVS-gestreamten virtuellen Desktops für einen X-Brick erforderlichen Ressourcen für Desktopvirtualisierung, Server, Netzwerk, Speicher und Datensicherheit.

Obwohl die Desktopvirtualisierungs-Infrastrukturkomponenten der Lösung in Abbildung 3 dafür entwickelt wurden, auf einer VSPEX Private Cloud-Lösung angelegt zu werden, umfassen die Referenzarchitekturen keine Konfigurationsdetails für die zugrunde liegende Proven Infrastructure.

Informationen zur Konfiguration der erforderlichen Infrastrukturkomponenten finden Sie im VSPEX Proven Infrastructure-Leitfaden unter Grundlegende Dokumente.

VSPEX Proven Infrastructures

EMC hat gemeinsam mit den branchenführenden Anbietern von IT-Infrastrukturen eine vollständige Virtualisierungslösung entwickelt, die die Bereitstellung der Private Cloud und der virtuellen Citrix XenDesktop-Desktops beschleunigt. Mit VSPEX sind Kunden in der Lage, ihre IT-Transformation durch schnellere Bereitstellung, verbesserte Anwenderfreundlichkeit, größere Auswahl, höhere Effizienz und weniger Risiko zu beschleunigen, anstatt die Herausforderungen und die Komplexität der Erstellung einer eigenen IT-Infrastruktur angehen zu müssen.

Die VSPEX-Validierung durch EMC ermöglicht eine zuverlässige Performance und ermöglicht Kunden die Auswahl von Technologien, die ihre vorhandene oder neu erworbene IT-Infrastruktur nutzen und so den Planungs-, Dimensionierungs- und Konfigurationsaufwand vermeiden. VSPEX stellt eine virtuelle Infrastruktur für Kunden bereit, die die charakteristische Einfachheit von echten konvergierten Infrastrukturen und gleichzeitig mehr Auswahlmöglichkeiten bei den einzelnen Stack-Komponenten erreichen möchten.

VSPEX Proven Infrastructures, wie in Abbildung 1 gezeigt, sind modulare und virtualisierte Infrastrukturen, die von EMC validiert und von EMC VSPEX-Partnern bereitgestellt werden. Sie umfassen die Virtualisierungs-, Server-, Netzwerk-, Speicher- und Datensicherheitsebene. Partner können die Virtualisierungs-, Server- und Netzwerktechnologien auswählen, die am besten zur Umgebung eines Kunden passen. Gleichzeitig stellen die Speichersysteme der hoch verfügbaren EMC XtremIO- und VNX-Produktreihe und von EMC bereitgestellte Datensicherheitstechnologien die Speicher- und Datensicherheitsebene zur Verfügung.

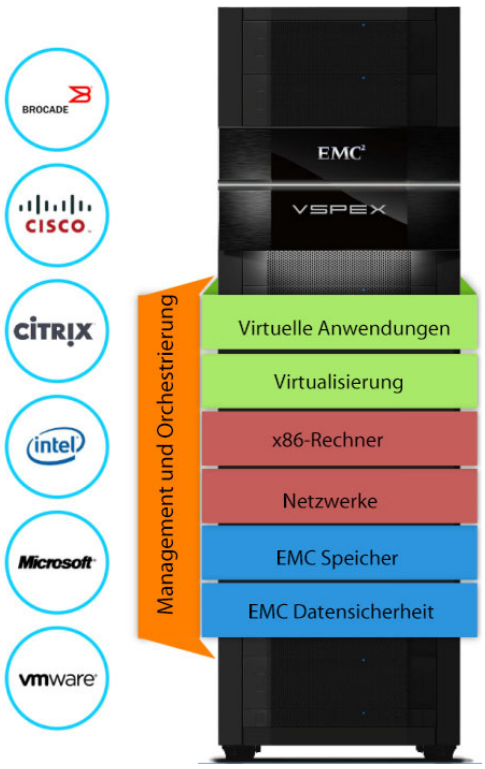

Abbildung 1. VSPEX Proven Infrastructures

Lösungsarchitektur

Allgemeine Architektur

Die EMC VSPEX-Lösung für Anwender-Computing für Citrix XenDesktop umfasst eine vollständige Systemarchitektur, die bis zu 1.750 MCS-verknüpfte Clones oder PVS-gestreamte virtuelle Desktops für einen Starter X-Brick und bis zu 3.500 MCS-verknüpfte Clones oder PVS-gestreamte virtuelle Desktops für einen X-Brick unterstützen kann. Die Lösung unterstützt Blockspeicher für virtuelle Desktops und optionale Dateispeicher für Benutzerdaten.

Abbildung 2 zeigt die übergeordnete Architektur der validierten Lösung.

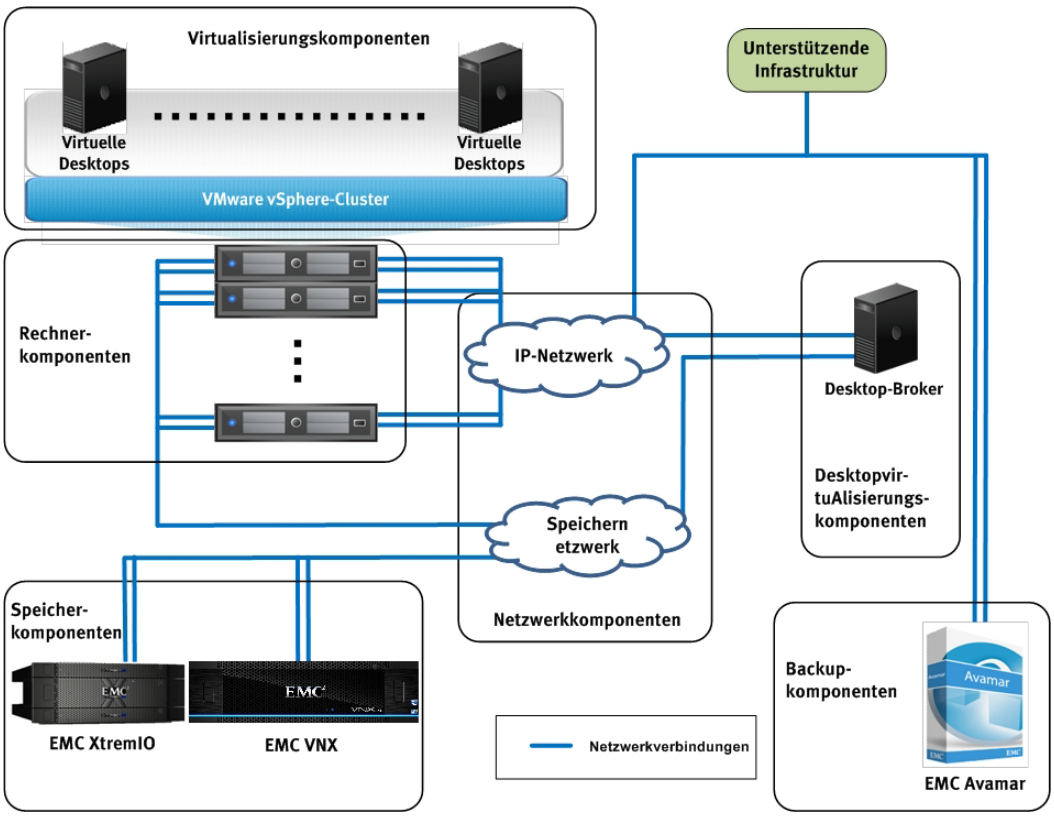

Abbildung 2. Architektur der validierten Lösung

Die Lösung verwendet EMC VNX und VMware vSphere für die Bereitstellung der Speicher- und Virtualisierungsplattformen für eine Citrix XenDesktop-Umgebung mit virtuellen, von MCS oder PVS bereitgestellten Microsoft Windows 8.1-Desktops.

Für die Lösung haben wir[1] das XtremIO-Array in mehreren Konfigurationen bereitgestellt, um bis zu 3.500 virtuelle Desktops zu unterstützen. Des Weiteren haben wir ein VNX-Array der nächsten Generation zum Hosten von Benutzerdaten bereitgestellt.

Das hoch verfügbare EMC XtremIO-Array stellt den Speicher für die Desktopvirtualisierungskomponenten bereit. Die Infrastrukturservices für die Lösung, die in Abbildung 3 dargestellt sind, können durch eine vorhandene Infrastruktur am Kundenstandort, durch die VSPEX Private Cloud oder durch die Bereitstellung der Services als dedizierte Ressourcen im Rahmen der Lösung bereitgestellt werden. Für die virtuellen Desktops, die in Abbildung 3 dargestellt werden, sind dedizierte Anwender-Computing-Ressourcen erforderlich. Eine Ausführung der Desktops in einer VSPEX Private Cloud ist nicht vorgesehen.

Die Planung und das Design der Speicherinfrastruktur für die Citrix XenDesktop-Umgebung ist ein wichtiger Schritt, da der gemeinsame Speicher in der Lage sein muss, große Belastungsspitzen bei I/O-Vorgängen abzufangen, die im Laufe eines Tages auftreten. Diese Belastungsspitzen können zu Phasen mit einer unregelmäßigen und unzuverlässigen Performance der virtuellen Desktops führen. Benutzer mögen sich an eine langsame Performance gewöhnen, aber eine unzuverlässige Performance führt zu Frustration und verringert die Effizienz.

[1] In diesem Leitfaden bezieht sich „wir“ auf das EMC Solutions Engineering-Team, das die Lösung validierte.

Für eine zuverlässige Performance von Anwender-Computing-Lösungen muss das Speichersystem die Spitzen-I/O-Last der Clients bei minimaler Antwortzeit verarbeiten können. Diese Lösung verwendet das EMC XtremIO-Array, um die von Kunden benötigten Antwortzeiten unter einer Millisekunde zu ermöglichen, während die Echtzeit-Inline-Deduplizierungsfunktionen der Plattform den benötigten physischen Speicher verringern. EMC Datensicherheits- und Recovery-Lösungen ermöglichen den Schutz von Benutzerdaten und die Wiederherstellbarkeit durch Anwender. Dafür werden in dieser Citrix XenDesktop-Lösung EMC Avamar und der damit verbundene Desktopclient verwendet.

Logische Architektur

Die EMC VSPEX-Lösung für Anwender-Computing für Citrix XenDesktop unterstützt Blockspeicher für die virtuellen Desktops. Abbildung 3 zeigt die logische Architektur der Lösung.

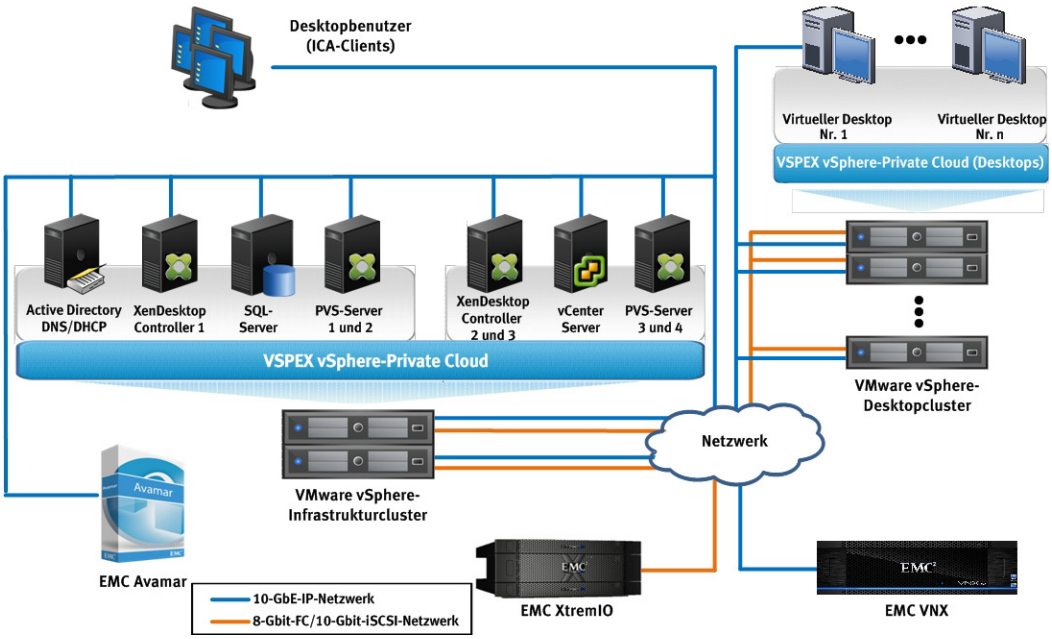

Abbildung 3. Logische Architektur für Block- und Filespeicher

Diese Lösung verwendet zwei Netzwerke: ein Speichernetzwerk zur Übertragung von virtuellen Desktop- und virtuellen Serverbetriebssystemdaten sowie ein 10-Gbit-Ethernetnetzwerk für den übrigen Datenverkehr. Für das Speichernetzwerk wird 8-Gbit-FC, 10-Gbit-CEE mit FCoE oder 10-Gbit-Ethernet mit iSCSI-Protokoll verwendet.

Hinweis: Diese Lösung unterstützt darüber hinaus 1-Gbit-Ethernet, falls die Bandbreitenanforderungen erfüllt werden.

Übersicht über die Kernkomponenten

In Tabelle 5 fasst die in dieser Lösung verwendeten zentralen Ebenen zusammen. Der Implementierungsleitfaden bietet einen Überblick über die einzelnen Komponenten.

Tabelle 5. Komponenten der VSPEX-Lösung

VSPEX-Ebene	Komponenten
Anwendungsebene	Citrix XenDesktop 7.1 mit: • Receiver • Storefront • Studio • Delivery Controller • Virtual Delivery Agent (VDA) • Maschinen mit Serverbetriebssystem • Maschinen mit Desktopbetriebssystem • PC-Remotezugriff • Lizenzserver • Citrix Machine Creation Services (MCS) • Citrix Provisioning Services (PVS) • Citrix Personal vDisk (PvDisk oder PvD) • Citrix Profile Management
Virtualisierungsebene	VMware vSphere-Hypervisor mit: • VMware vSphere • VMware vCenter Server • VMware vSphere-Hochverfügbarkeit • EMC VSI (Virtual Storage Integrator)
Rechnerebene	VSPEX definiert die Mindestanzahl der für die Rechnerebene erforderlichen Ressourcen. Der Kunde hat jedoch die Möglichkeit, jede beliebige Serverhardware zu implementieren, die diese Anforderungen erfüllt.
Netzwerkebene	VSPEX definiert die Mindestanzahl der für die Lösung benötigten Netzwerkports und stellt allgemeine Richtlinien zur Netzwerkarchitektur bereit. Der Kunde hat jedoch die Möglichkeit, jede beliebige Netzwerkhardware zu implementieren, die diese Anforderungen erfüllt.

VSPEX-Ebene	Komponenten
Speicherebene	EMC XtremIO-Serie mit: • EMC XtremIO Management Server • EMC Virtual Storage Integrator (VSI) for VMware vSphere • VMware vSphere Storage APIs for Array Integration • EMC XtremIO Snapshots EMC VNX-Serie der nächsten Generation mit: • EMC Unisphere Management Suite • EMC Virtual Storage Integrator (VSI) for VMware vSphere • VMware vSphere Storage APIs for Array Integration • VMware vSphere Storage APIs for Storage Awareness • EMC VNX Snapshots • EMC SnapSure™ • EMC VNX Virtual Provisioning • EMC FAST Suite: FAST Cache und Fully Automated Storage Tiering for Virtual Pools (FAST VP)
Datensicherheitsebene	EMC Avamar
Sicherheitsebene	RSA SecurID

Kapitel 4 Lösungsimplementierung

In diesem Kapitel werden die folgenden Themen behandelt:

Übersicht 28

Netzwerkimplementierung 29

Vorbereiten und Konfigurieren der Speicherarrays 32

Installieren und Konfigurieren der vSphere-Hosts 41

Installieren und Konfigurieren der SQL Server-Datenbank 44

Bereitstellen von VMware vCenter Server 45

Installieren und Konfigurieren der XenDesktop Delivery Controller 46

Installieren und Konfigurieren von Citrix Provisioning Services 49

Einrichten von EMC Avamar 53

Übersicht

In diesem Kapitel wird beschrieben, wie die Referenzarchitektur der Anwender-Computing-Lösung implementiert wird. Wenn Sie bereits über eine VSPEX Proven Infrastructure-Umgebung verfügen, können Sie Abschnitte mit den schon abgeschlossenen Schritten für die Implementierung überspringen.

Andernfalls finden Sie Informationen zur Konfiguration der erforderlichen Infrastrukturkomponenten in dem unter Grundlegende Dokumente aufgelisteten VSPEX Proven Infrastructure-Leitfaden.

Hinweis: Diese Lösung erfordert bestimmte Infrastrukturservices, die in Abbildung 3 dargestellt sind. Diese können durch eine vorhandene Infrastruktur am Kundenstandort, durch eine VSPEX Private Cloud oder durch die Bereitstellung der Services als dedizierte Ressourcen im Rahmen dieser Lösung bereitgestellt werden.

In Tabelle 6 listet die Hauptphasen des Implementierungsprozesses der Lösung auf und stellt Links zu den relevanten Abschnitten in diesem Kapitel bereit.

Tabelle 6. Überblick über den Implementierungsprozess

Phase	Beschreibung	Referenz
1	Konfigurieren der Switche und Netzwerke und Verbinden mit dem Kundennetzwerk	Netzwerkimplementierung
2	Installation und Konfiguration der XtremIO- und VNX-Arrays	Vorbereiten und Konfigurieren der Speicherarrays
3	Konfigurieren der Datastores der virtuellen Maschinen	Vorbereiten und Konfigurieren der Speicherarrays
4	Installieren und Konfigurieren der Server	Installieren und Konfigurieren der vSphere-Hosts
5	Einrichten von SQL Server (verwendet von vCenter, XenDesktop und Citrix Provisioning Services)	Installieren und Konfigurieren der SQL Server-Datenbank
6	Installieren und Konfigurieren von vCenter und des Netzwerks der virtuellen Maschine	Installieren und Konfigurieren der vSphere-Hosts
7	Einrichten der XenDesktop Delivery Controller	Installieren und Konfigurieren der XenDesktop Delivery Controller
8	Einrichten von Citrix Provisioning Services (PVS)	Installieren und Konfigurieren von Citrix Provisioning Services
9	Einrichten von EMC Avamar	Einrichten von EMC Avamar

Netzwerkimplementierung

In diesem Abschnitt werden die Anforderungen für die Vorbereitung der Netzwerkinfrastruktur beschrieben, die zur Unterstützung dieser Lösung erforderlich ist. In Tabelle 7 enthält eine Zusammenfassung der abzuschließenden Aufgaben sowie Referenzen zu weiteren Informationen.

Tabelle 7. Aufgaben für die Switch- und Netzwerkkonfiguration

Aufgabe	Beschreibung	Referenz
Konfigurieren des Infrastrukturnetzwerks	Konfigurieren Sie das Speicherarray und das vSphere-Hostinfrastrukturnetzwerk.	Konfigurieren des Infrastrukturnetz-werks
Konfigurieren der virtuellen LANs	Konfigurieren Sie private und öffentliche virtuelle LANs nach Bedarf.	Konfigurationsleitfaden Ihres Switch-Anbieters
Konfigurieren Sie das Speichernetzwerk.	Konfigurieren Sie die FC/FCoE-Switchports, das Zoning für vSphere-Hosts und das Speicherarray.	• Konfigurieren des Speichernetzwerks • Konfigurationsleitfaden Ihres Switch-Anbieters
Vervollständigen der Netzwerkverkabelung	Verbinden Sie die Switchverbindungsports, VNX-Ports und vSphere-Serverports.	Verkabeln des Netzwerks

Konfigurieren des Infrastrukturnetz-werks

Das Infrastrukturnetzwerk erfordert redundante Netzwerkverbindungen für jeden vSphere-Host, das Speicherarray, die Switch-Verbindungsports und die Switch-Uplink-Ports. Diese Konfiguration stellt sowohl Redundanz als auch zusätzliche Netzwerkbandbreite bereit.

Diese Konfiguration ist unabhängig davon erforderlich, ob die Netzwerkinfrastruktur für die Lösung bereits vorhanden ist oder zusammen mit anderen Komponenten der Lösung bereitgestellt wird.

Abbildung 4 zeigt ein Beispiel einer redundanten Ethernetinfrastruktur für die dieser Lösung verwendeten VNX. Diese Lösung verwendet redundante Switche und Verbindungen, um sicherzustellen, dass kein Single-Point-of-Failure in der Netzwerkverbindung vorhanden ist.

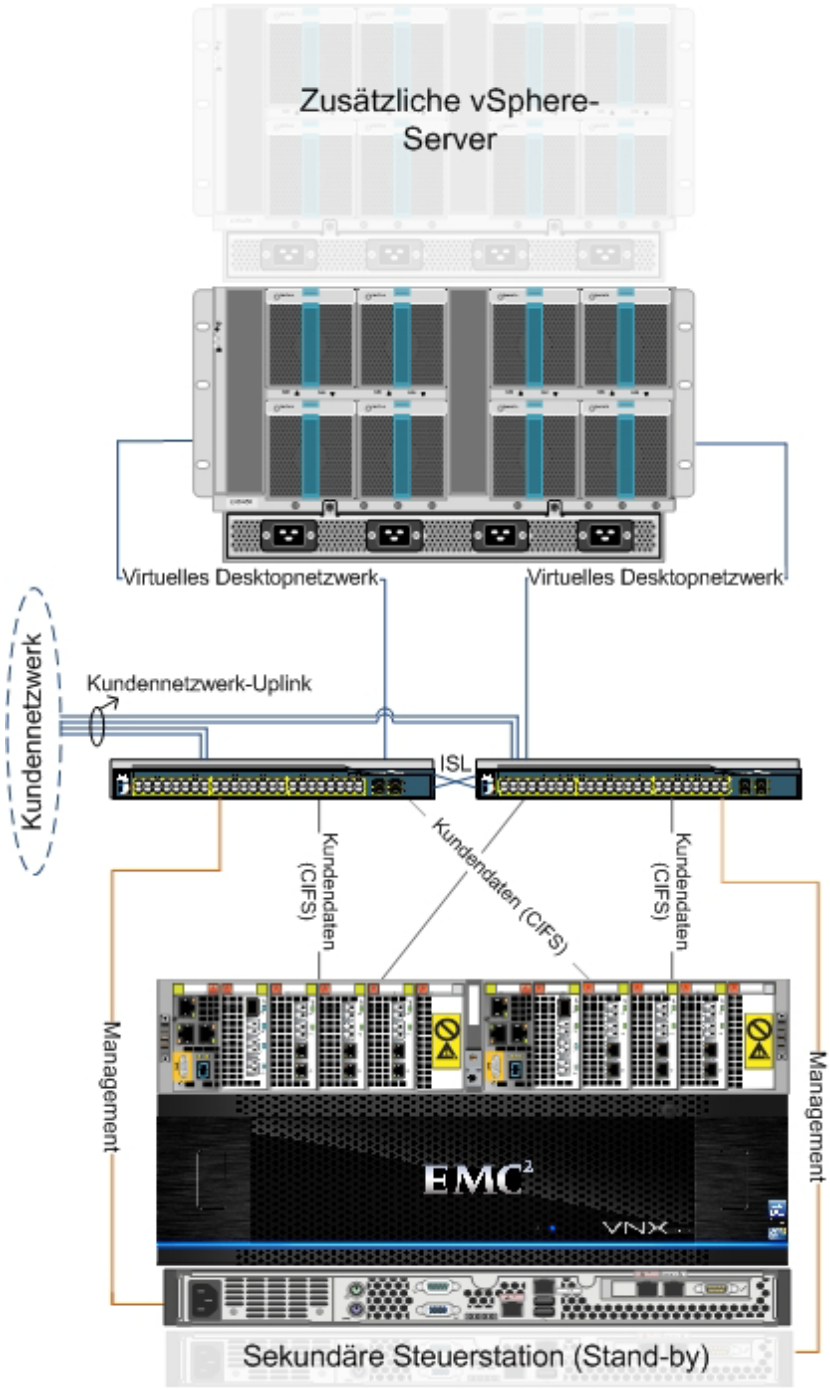

Abbildung 4. Beispiel-Ethernetnetzwerkarchitektur

Konfiguration der VLANs

Stellen Sie sicher, dass es entsprechende Switchports für das Speicherarray und vSphere-Hosts gibt. EMC empfiehlt, die vSphere-Hosts mit mindestens zwei virtuellen LANs zu konfigurieren:

- **Clientzugriffsnetzwerk**: Netzwerk der virtuellen Maschinen und CIFS-Datenverkehr (Common Internet File System). Dies sind kundenorientierte Netzwerke, die bei Bedarf getrennt werden können.
- **Managementnetzwerk:** vSphere-Management und VMware vMotion (privates Netzwerk)

Konfigurieren des Speichernetzwerks

Diese Lösung benötigt ein dediziertes Speichernetzwerk. Wenn iSCSI verwendet wird, um das XtremIO-Array mit vSphere-Hosts zu verbinden, ist ein dediziertes VLAN für das Speichernetzwerk erforderlich. Wenn Fibre Channel (FC) oder eine Kombination aus FC für das XtremIO-Array und FCoE für die vSphere-Hosts verwendet wird, sind keine weiteren virtuellen LANs für das Speichernetzwerk erforderlich.

Für die Lösungstests haben wir ein FC-Netzwerk verwendet. Für das Infrastruktur-Fibre-Channel-Netzwerk sind redundante Fibre-Channel-Switches sowie Links für jeden vSphere-Host und das Speicherarray erforderlich. Diese Konfiguration stellt sowohl Redundanz als auch zusätzliche Speichernetzwerkbandbreite bereit. Wir haben jeden vSphere-Host mit beiden Fibre-Channel-Switches und jeden Switch mit jedem Speicherprozessor auf dem Speicher-Array verbunden. Wir haben dann jede der Fibre-Channel-Verbindungen zwischen dem vSphere-Host und dem Speicher-Array in eine separate Fibre-Channel-Zone platziert.

Abbildung 5 zeigt die für das Testen dieser Lösung verwendete Netzwerkarchitektur.

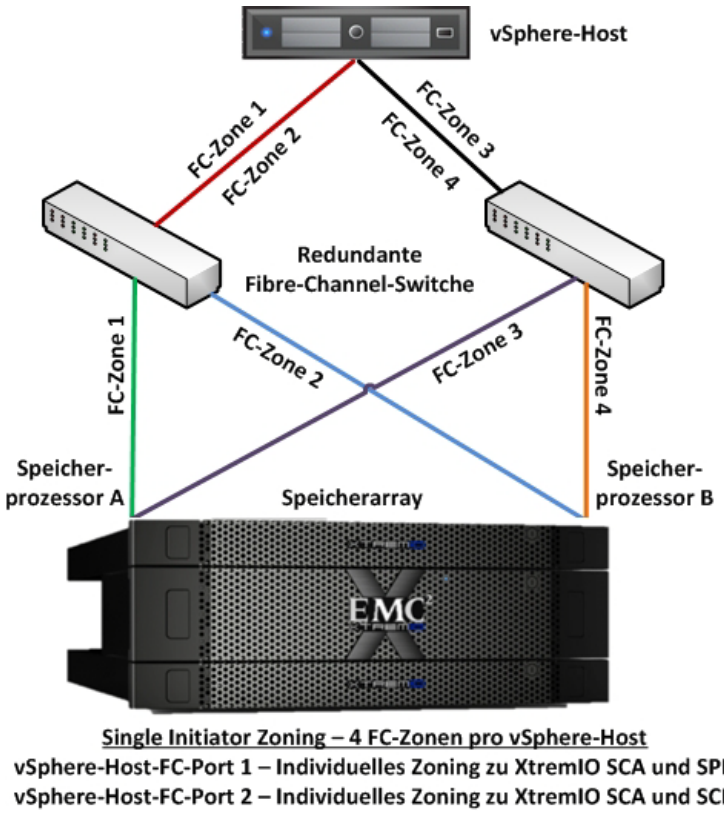

Abbildung 5. Beispiel für eine Fibre-Channel-Netzwerkarchitektur

Verkabeln des Netzwerks

Sorgen Sie dafür, dass alle Lösungsserver, Speicher-Arrays, Switch-Verbindungen und Switch Uplinks über redundante Verbindungen verfügen und in separate Switching-Infrastrukturen eingesteckt sind. Sorgen Sie auch dafür, dass eine vollständige Verbindung zum vorhandenen Kundennetzwerk besteht.

Hinweis: An diesem Punkt wird die neue Hardware mit dem vorhandenen Kundennetzwerk verbunden. Achten Sie darauf, dass unvorhergesehene Interaktionen keine Serviceprobleme im Kundennetzwerk hervorrufen.

Vorbereiten und Konfigurieren der Speicherarrays

In diesem Abschnitt wird die Konfiguration des VNX-Speicherarrays beschrieben. In dieser Lösung stellt VNX NFS- oder VMFS-Datenspeicher (VMware Virtual Machine File System) für VMware-Hosts bereit. In Tabelle 8 zeigt die Aufgaben für die Speicherkonfiguration.

Tabelle 8. Aufgaben für die Speicherkonfiguration

Aufgabe	Beschreibung	Referenz
Vorbereiten und Installieren von XtremIO	Installieren Sie die XtremIO-Hardware gemäß der Produktdokumentation.	*EMC XtremIO-Speicherarray – Handbuch zur Hardwareinstallation und Upgrade*
Einrichten der XtremIO-Erstkonfiguration	Konfigurieren Sie die IP-Adressinformationen und andere wichtige Parameter auf dem XtremIO-Array.	*EMC XtremIO-Speicherarray – Handbuch zur Softwareinstallation und Upgrade*
Konfigurieren von XtremIO-Ereignishandlern	Konfigurieren Sie XtremIO-Ereignishandler so, dass Benachrichtigungen in Bezug auf die Auslastung des physischen Arrayspeichers gesendet werden.	Konfigurieren von XtremIO-Ereignishandlern
Speicher-Provisioning für VMFS-Datastores	Erstellen Sie XtremIO-Volumes, die den vSphere-Servern als VMFS-Datastores angezeigt werden, die die virtuellen Desktops hosten.	Speicher-Provisioning für VMFS-Datastores
Vorbereiten der VNX	Installieren Sie die VNX-Hardware gemäß der Produktdokumentation.	*VSPEX Private Cloud Proven Infrastructure-Leitfaden*
Einrichten der VNX-Erstkonfiguration	Konfigurieren Sie die IP-Adressinformationen und andere wichtige Parameter auf der VNX.	*VSPEX Private Cloud Proven Infrastructure-Leitfaden*
Konfigurieren von VNX Fast Cache	Konfigurieren Sie FAST Cache. Konfigurieren Sie optional FAST VP.	Konfigurieren von VNX Fast Cache Konfigurieren von FAST VP für Benutzerdaten (optional)

Aufgabe	Beschreibung	Referenz
Provisioning von optionalem VNX-Speicher für Benutzerdaten	Erstellen Sie CIFS-Dateisysteme, die zum Speichern von Roaming-Benutzerprofilen und Stammverzeichnissen verwendet werden. Konfigurieren Sie FAST Cache. Konfigurieren Sie optional FAST VP.	Provisioning von optionalem VNX-Speicher für Benutzerdaten
Anforderungen der VSPEX Private Cloud	Erstellen Sie zusätzliche VMFS-Datastores, um SQL-Server, Domain-Controller, vCenter-Server, Citrix XenDesktop Delivery Controller und die virtuellen Maschinen von Citrix Provisioning Services zu hosten.	Speicherlayout

Vorbereiten und Installieren von XtremIO

Für diese Lösung gibt es keine spezifischen Konfigurationsschritte. Anweisungen für Zusammenstellung, Rackeinbau, Verkabelung und Stromversorgung für das XtremIO-Array finden Sie in den folgenden Dokumenten:

- *EMC XtremIO-Speicherarray – Handbuch zur Vorbereitung des Aufstellorts*
- *EMC XtremIO-Speicherarray – Checkliste für Aufgaben vor der Installation*
- *EMC XtremIO-Speicherarray – Handbuch zur Softwareinstallation und Upgrade*
- *EMC XtremIO-Speicherarray – Handbuch zur Hardwareinstallation und Upgrade*

Einrichten der XtremIO-Erstkonfiguration

Konfigurieren Sie nach der Vorbereitung der XtremIO wichtige Informationen zur vorhandenen Umgebung, damit das Speicherarray kommunizieren kann. Konfigurieren Sie die folgenden allgemeinen Elemente gemäß den für Ihr IT-Rechenzentrum geltenden Richtlinien und vorhandenen Infrastrukturinformationen.

- Domain Name System (DNS)
- Network Time Protocol (NTP)
- XMS-Netzwerkschnittstelle
- Schnittstellen des Speichernetzwerks
- IP-Adressen des Speichernetzwerks

Konfigurieren von XtremIO-Ereignishandlern

Sie können XtremIO so konfigurieren, dass Ihnen Warnmeldungen per E-Mail zugesendet werden, wenn Ereignisse der Kategorie **Software** – **Minor** – **Cluster** auftreten, eine Klassifizierung, die Ereignisse umfasst, die mit clusterfreier Kapazität in Verbindung stehen. Eine vollständige Liste von XtremIO-Fehlern und -Warnungen finden Sie im *EMC XtremIO-Speicherarray – Benutzerhandbuch*.

Um einen Ereignishandler zu erstellen, um per E-Mail benachrichtigt zu werden, wenn diese Ereignisse auftreten, führen Sie die folgenden Schritte aus:

1. Klicken Sie in der XtremIO Storage Management Application auf das Symbol **Alerts & Events**.
2. Klicken Sie im Fenster **Alerts & Events** auf **Events**.

3. Klicken Sie oben rechts auf die Schaltfläche **Display Event Handlers**, wie in Abbildung 6 dargestellt.

Abbildung 6. Schaltfläche „XtremIO Display Event Handlers“

4. Klicken Sie im Fenster **Event Handlers** auf **Add**.
5. Wählen Sie im Fenster **Add Event Handler** Folgendes aus, wie in Abbildung 7 dargestellt, wobei sich Cluster auf den Namen des XtremIO-Clusters bezieht, der bei der Installation angegeben wurde:
   - Kategorie: **Software**
   - Schweregrad: **Minor**
   - Entität: **Cluster**
   - Details zur Entität: **‹cluster name›**
6. Aktivieren Sie im selben Fenster das Kontrollkästchen **Send e-mail** und klicken Sie dann auf **OK.** Die Warnmeldung kann auch mit den Optionen **Send SNMP Trap** oder **Send to Syslog** konfiguriert werden.

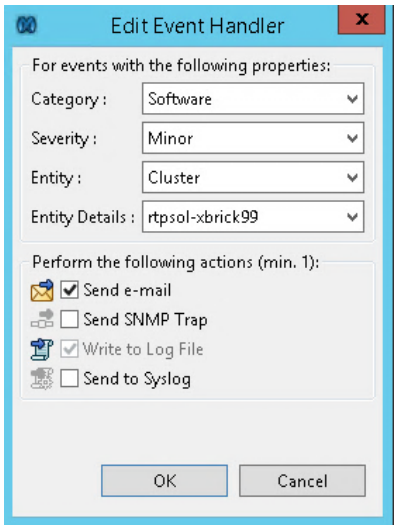

Abbildung 7. XtremIO-Fenster „Edit Event Handler“

7. Klicken Sie in der XtremIO Storage Management Application auf das Symbol **Administration**.
8. Klicken Sie auf der Registerkarte **Administration** - **Email Configuration** auf **Add**, um alle E-Mail-Adressen hinzuzufügen, die Kopien von XtremIO-Warnmeldungen erhalten sollen. Wenn Sie den Ereignishandler so konfiguriert haben, dass entweder SNMP oder Syslog für das Senden von Warnmeldungen verwendet wird, müssen Sie diese Optionen konfigurieren, sofern Sie sie noch nicht auf den Registerkarten **SNMP Configuration** oder **Syslog Configuration** konfiguriert haben.

Speicher-Provisioning für VMFS-Datastores

Führen Sie in der EMC XtremIO Storage Management Application die folgenden Schritte aus, um die Volumes auf dem XtremIO-Array für die Speicherung von virtuellen Desktops zu konfigurieren:

Führen Sie die folgenden Schritte aus, um die erforderlichen Volumes zu konfigurieren, wie unter Tabelle 9 beschrieben, und sie den vSphere-Servern als VMFS-Datastores anzuzeigen. Es werden zwei Datastore-Konfigurationen für jeden Desktoptyp aufgelistet: eine Konfiguration mit dem Speicherplatz, der für die Verwendung der Citrix Personal vDisk (PvD)-Funktion erforderlich ist, und eine, die diese Citrix XenDesktop-Komponente nicht verwendet. Beachten Sie bei der Bereitstellung von Citrix-Desktops über PVS, dass die folgenden Werte standardmäßig konfiguriert sind:

- PVS-Schreibcachelaufwerk: 6 GB
- Citrix Personal vDisk (PvD): 10 GB

Wenn einer dieser Standardwerte geändert wird, müssen auch die Datastore-Größen entsprechend geändert werden.

Tabelle 9. Volumes auf der XtremIO zum Speichern virtueller Desktops

XtremIO-Konfiguration	Anzahl der Desktops	Desktoptyp	Anzahl Volumes	Größe des Volumes
Starter X-Brick	1.750	PVS-gestreamt	7	2.500 GB
		PVS-gestreamt mit PvD		5.000 GB
		MCS-verknüpfter Clone	14	750 GB
		MCS-verknüpfter Clone mit PvD		2.000 GB
X-Brick	3.500	PVS-gestreamt	14	2.500 GB
		PVS-gestreamt mit PvD		5.000 GB
		MCS-verknüpfter Clone	28	750 GB
		MCS-verknüpfter Clone mit PvD		2.000 GB

1. Klicken Sie auf **Configuration**.
2. Klicken Sie im Bereich **Volume** auf **Add**.
3. Klicken Sie im Fenster **Add New Volumes** auf **Add Multiple**.
4. Geben Sie im Feld **Number of Volumes** die erforderliche Anzahl der Datastores ein, basierend auf der Konfiguration und der Anzahl der virtuellen Desktops. Geben Sie im Feld **Name** einen Namen für das gemeinsame LUN und im Feld **Size** je nach Bedarf 750 GB oder 5000 GB ein und klicken Sie dann auf **Ok**.

Vorbereiten der VNX

Für diese Lösung gibt es keine spezifischen Konfigurationsschritte. Anweisungen für Montage, Rackaufbau, Verkabelung und Stromanschluss des VNX-Arrays finden Sie im *EMC Installationshandbuch für VNX5400* Unified.

Einrichten der VNX-Erstkonfiguration

Konfigurieren Sie nach der Vorbereitung der VNX wichtige Informationen zur vorhandenen Umgebung, damit das Speicherarray kommunizieren kann. Konfigurieren Sie die folgenden allgemeinen Elemente gemäß den für Ihr IT-Rechenzentrum geltenden Richtlinien und vorhandenen Infrastrukturinformationen.

- Domain Name System (DNS)
- Network Time Protocol (NTP)
- Schnittstellen des Speichernetzwerks
- IP-Adresse des Speichernetzwerks
- CIFS-Services und Active Directory-Domain-Mitgliedschaft

Weitere Informationen zum Konfigurieren der VNX-Plattform finden Sie in den in Tabelle 8 aufgelisteten Referenzdokumenten. Informationen zum Laufwerkslayout finden Sie im Designleitfaden.

Konfigurieren von VNX Fast Cache

Führen Sie in Unisphere die folgenden Schritte aus, um FAST Cache auf dem VNX-Speicherpool für diese Lösung zu konfigurieren.

1. So zeigen Sie weitere Informationen zu FAST Cache für das VNX-Array an:
   a. Klicken Sie in Unisphere auf **Properties** und wählen Sie **Manage Cache** aus.
   b. Wechseln Sie im Dialogfeld **Storage System Properties**, wie in Abbildung 8 dargestellt, zur Registerkarte **FAST Cache**, um Informationen zu FAST Cache anzuzeigen.

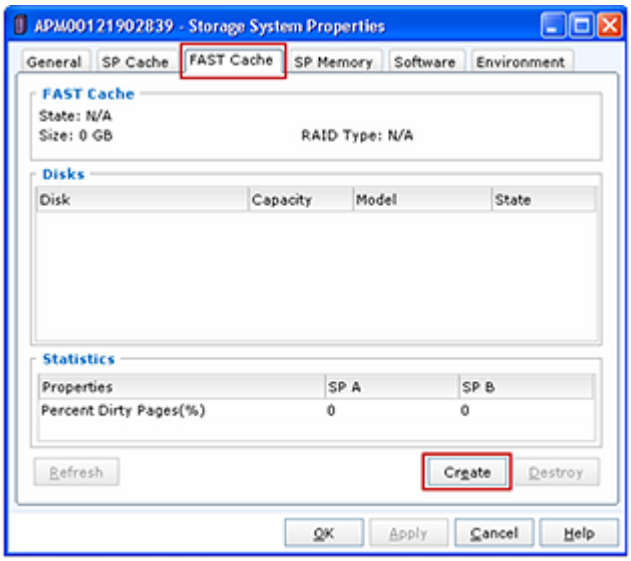

Abbildung 8. Dialogfeld Storage System Properties

2. So erstellen Sie FAST Cache:

   a. Klicken Sie auf **Create**, um das Dialogfeld **Create FAST Cache** zu öffnen, wie in Abbildung 9 gezeigt.

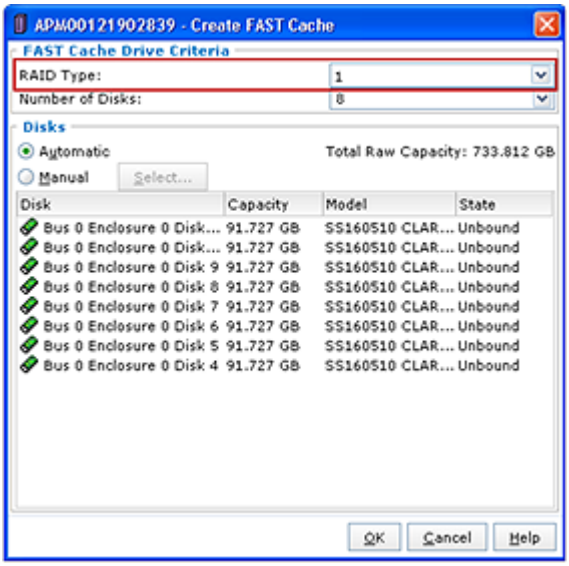
APM00121902839 - Create FAST Cache
FAST Cache Drive Criteria
RAID Type:
1
Number of Disks:
8
Disks
Automatic
Total Raw Capacity: 733.812 GB
Manual
Select...
Disk
Capacity
Model
State
Bus 0 Enclosure 0 Disk... 91.727 GB SS160510 CLAR... Unbound
Bus 0 Enclosure 0 Disk... 91.727 GB SS160510 CLAR... Unbound
Bus 0 Enclosure 0 Disk 9 91.727 GB SS160510 CLAR... Unbound
Bus 0 Enclosure 0 Disk 8 91.727 GB SS160510 CLAR... Unbound
Bus 0 Enclosure 0 Disk 7 91.727 GB SS160510 CLAR... Unbound
Bus 0 Enclosure 0 Disk 6 91.727 GB SS160510 CLAR... Unbound
Bus 0 Enclosure 0 Disk 5 91.727 GB SS160510 CLAR... Unbound
Bus 0 Enclosure 0 Disk 4 91.727 GB SS160510 CLAR... Unbound
OK
Cancel
Help

Abbildung 9. Erstellen des FAST Cache-Dialogfelds

   b. Wählen Sie die erforderliche Anzahl der Laufwerke aus, die für FAST Cache verwendet werden sollen.

Hinweis: Informationen zum Bestimmen der in dieser Lösung erforderlichen Anzahl von Flashlaufwerken finden Sie im Designleitfaden.

---

   c. Wenn die Option **Automatic** ausgewählt ist, werden die für die Erstellung von FAST Cache verwendeten Flashlaufwerke im Dialogfeld angezeigt.

   Mit der Option **Manual** können Sie die Laufwerke manuell auswählen.

   d. Klicken Sie auf **OK**, um FAST Cache mithilfe der ausgewählten Laufwerke zu erstellen.

Hinweis: Wenn keine ausreichende Anzahl an Flashlaufwerken verfügbar ist, wird eine Fehlermeldung angezeigt und FAST Cache kann nicht erstellt werden.

---

   e. Aktivieren Sie FAST Cache für den Speicherpool, der für die Lösung erstellt wurde.

   – FAST Cache wird nach der Erstellung standardmäßig für alle neuen Pools aktiviert.

   – Um FAST Cache für einen vorhandenen Pool zu aktivieren, wählen Sie **im Dialogfeld Storage Pool Properties unter Advanced die Option FAST Cache Enabled aus.**

Die FAST Cache-Funktion der VNX führt nicht zu einer sofortigen Performanceverbesserung. Das System muss Daten zu Zugriffsmustern sammeln und häufig verwendete Informationen in den Cache hochstufen. Dieser Vorgang dauert einige Stunden, in denen die sich Performance des Arrays stetig verbessert.

Provisioning von optionalem VNX-Speicher für Benutzerdaten

Wenn in der Produktionsumgebung der erforderliche Speicher für Benutzerdaten (d. h. Roaming-Benutzerprofile oder XenDesktop Profile Management-Repositories und Stammverzeichnisse) nicht vorhanden ist und die optionale Benutzerdatenspindel erworben wurde, führen Sie in Unisphere die folgenden Schritte aus, um zwei CIFS-Dateisysteme auf VNX zu konfigurieren:

1. Erstellen Sie einen blockbasierten RAID-6-Speicherpool mit den in Tabelle 10 gezeigten Merkmalen.

Tabelle 10. Erstellen eines blockbasierten RAID 6-Speicherpools

Konfiguration	Anzahl der Laufwerke	Laufwerkstyp
1.750 virtuelle Desktops	24	2 TB NL-SAS
3.500 virtuelle Desktops	48	

Im Designleitfaden werden die Speicherlayouts beschrieben.

2. Stellen Sie die erforderlichen LUNs aus dem Pool zur Verfügung, wie in Tabelle 11 gezeigt, die dem Data Mover als Dvols eines systemdefinierten NAS-Pools angezeigt werden.

Tabelle 11. Konfigurieren von LUNs für NAS-Pools

Konfiguration	Anzahl an LUNs	LUN-Größe (TB)
1.750 virtuelle Desktops	10	2,25
3.500 virtuelle Desktops	20	2,25

3. Stellen Sie vier Dateisysteme aus dem NAS-Pool zum Exportieren als CIFS-Shares auf einem CIFS-Server bereit.

Für Konfigurationen mit 3.500 Desktops müssen die Dateisysteme auf zwei CIFS-Server verteilt werden. Darüber hinaus müssen die CIFS-Server auf die beiden aktiven Data Mover auf der VNX5400 verteilt werden.

Konfigurieren von FAST VP für Benutzerdaten (optional)

Sie können FAST VP optional so konfigurieren, dass die Datenverschiebung zwischen Storage Tiers im Speicherpool für Benutzerdaten automatisiert wird. Sie können FAST VP auf Pool- oder LUN-Ebene konfigurieren.

Konfigurieren von FAST VP auf Poolebene

Wählen Sie zum Anzeigen und Managen von FAST VP auf Poolebene den Speicherpool für die Benutzerdaten aus und klicken Sie auf **Properties**, um das Dialogfeld **Storage Pool Properties** zu öffnen.

Tier Status zeigt FAST-VP-Verlagerungsinformationen an, die für den ausgewählten Pool spezifisch sind. **Tier Details** zeigt die genaue Verteilung der Daten an.

Abbildung 10 zeigt die Tiering-Informationen für einen bestimmten FAST VP-aktivierten Pool.

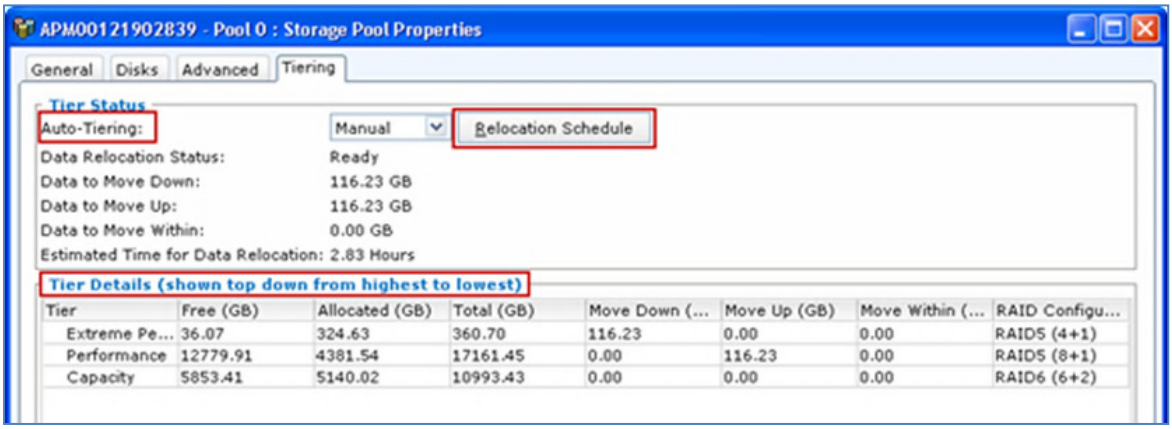

Abbildung 10. Dialogfeld Storage Pool Properties

Sie können die geplante Verlagerung auf der Poolebene aus dem Menü **Auto-Tiering** auswählen. Sie können zwischen den Optionen **Automatic** und **Manual** auswählen. Klicken **Sie auf Relocation Schedule, um** das Fenster **Manage Auto-Tiering** zu **öffnen, wie in** Abbildung 11 **dargestellt. In diesem Fenster können Sie die Datenverlagerung**srate steuern. Standardmäßig ist die Rate mit dem Wert **Medium** auf Mittel eingestellt, sodass die Host-I/O-Vorgänge nicht wesentlich beeinträchtigt sind.

Hinweis: FAST VP ist ein vollständig automatisiertes Tool, d. h., Verlagerungen können automatisch ausgeführt werden. EMC empfiehlt, Verlagerungen außerhalb der Spitzenzeiten zu planen, um potenzielle Performanceeinbußen zu vermeiden.

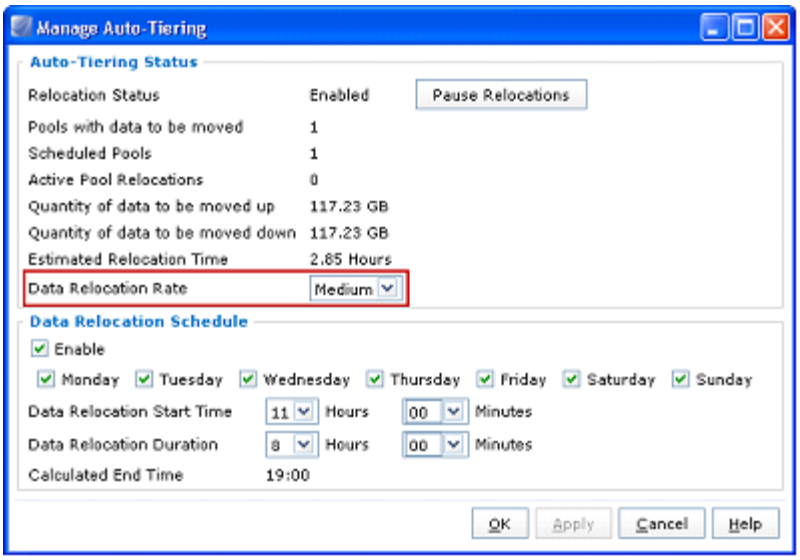

Abbildung 11. Das Fenster „Manage Auto-Tiering“

Anforderungen der VSPEX Private Cloud

Diese VSPEX Proven Infrastructure für Anwender-Computing erfordert mehrere Anwendungsserver. Sofern nicht anders angegeben, verwenden alle Server Microsoft Windows Server 2012 R2 als Betriebssystem. In Tabelle 12 listet die Mindestanforderungen jedes erforderlichen Infrastrukturservers auf.

Tabelle 12. Mindestanforderungen für den Infrastrukturserver

Server	CPU	RAM	IOPS	Speicherkapazität
Domain-Controller (je)	2 vCPUs	4 GB	25	32 GB
SQL Server	2 vCPUs	6 GB	100	200 GB
vCenter Server	4 vCPUs	8 GB	100	80 GB
Citrix XenDesktop-Controller (jeweils)	2 vCPUs	8 GB	50	32 GB

Speicherlayout der Private Cloud

Diese Lösung erfordert ein Volume mit 1,5 TB zum Hosten der virtuellen Infrastrukturmaschinen, die VMware vCenter Server, Citrix XenDesktop-Controller, Citrix PVS-Server, optionale Citrix ShareFile-Server, Microsoft Active Directory Server und Microsoft SQL-Server umfassen können.

Anforderungen von Citrix ShareFile

In Tabelle 13 sind die Mindestanforderungen für CPU und Arbeitsspeicher für eine Implementierung von Citrix ShareFile StorageZones mit Storage Center aufgeführt.

Tabelle 13. Minimum der Hardwareressourcen für ShareFile StorageZones mit Storage Center

CPU (Kerne)	Arbeitsspeicher (GB)	Referenz
2	4	*Storage Center system requirements* auf der Citrix eDocs-Website.

Citrix ShareFile-Speicherlayout

Für ShareFile StorageZones ist eine CIFS-Share zur Bereitstellung des privaten Datenspeichers für Storage Center erforderlich. Die VNX, die den Speicher für VSPEX-Lösungen für Anwender-Computing bereitstellt, bietet File- und Blockzugriff sowie umfassende Funktionen und ist die ideale Wahl für ShareFile StorageZones-Bereitstellungen. In Tabelle 14 zeigt den empfohlenen VNX-Speicher für die CIFS-Share für StorageZones.

Tabelle 14. Empfohlener VNX-Speicher der CIFS-Share für ShareFile StorageZones

CIFS-Share für (Anzahl der Benutzer)	Konfiguration	Anmerkungen
1750 Anwender	24 3,5-Zoll-NL-SAS-Laufwerke mit 2 TB und 7.200 U/min. (6+2 RAID 6)	Für diese Konfiguration wird vorausgesetzt, dass jeder Benutzer über 10 GB an privatem Speicherplatz verfügt.
3.500 Anwender	48 3,5-Zoll-NL-SAS-Laufwerke mit 2 TB und 7.200 U/min. (6+2 RAID 6)	

Installieren und Konfigurieren der vSphere-Hosts

In diesem Abschnitt finden Sie Informationen zur Installation und Konfiguration der vSphere-Hosts und Infrastrukturserver, die zur Unterstützung der Architektur erforderlich sind. In Tabelle 15 beschreibt die Aufgaben, die abgeschlossen werden müssen.

Tabelle 15. Aufgaben für die Serverinstallation

Aufgabe	Beschreibung	Referenz
Installieren von vSphere	Installieren Sie den vSphere-Hypervisor auf den physischen Servern, die für die Lösung bereitgestellt werden.	*Installations- und Einrichtungshandbuch für vSphere*
Konfigurieren des vSphere-Netzwerks	Konfigurieren Sie das vSphere-Netzwerk, einschließlich NIC-Trunking (Netzwerkschnittstellenkarten), VMkernel-Ports und virtuellen Maschinenportgruppen.	*Handbuch für vSphere-Netzwerk* Konfigurieren des vSphere-Netzwerks
Hinzufügen von vSphere-Hosts zu XtremIO-Initiatorgruppen	Fügen Sie die vSphere-Hosts den Initiatorgruppen hinzu, die in Vorbereiten und Konfigurieren der Speicherarrays erstellt wurden.	EMC Online Support
Verbinden der VMware-Datenspeicher	Verbinden Sie die VMware-Datastores mit den für die Lösung bereitgestellten vSphere-Hosts.	*Handbuch für vSphere-Speicher* Verbinden von vSphere-Datastores
vSphere optimieren:	Nehmen Sie die erforderlichen Änderungen an der Konfiguration vor, um eine optimale Performance des XtremIO-Arrays sicherzustellen	*EMC XtremIO-Speicherarray – Benutzerhandbuch* Optimieren von vSphere für XtremIO

Installieren von vSphere

Bestätigen oder aktivieren Sie nach dem ersten Einschalten der für vSphere verwendeten Server die Einstellung für die hardwaregestützte CPU-Virtualisierung und die hardwaregestützte MMU-Virtualisierung im BIOS jedes Servers. Wenn die Server mit einem RAID-Controller ausgestattet sind, empfiehlt EMC, eine Spiegelung auf den lokalen Festplatten zu konfigurieren.

Starten Sie die vSphere-Installationsmedien, und installieren Sie den Hypervisor auf jedem der Server. Für die Installation sind vSphere-Hostnamen, IP-Adressen und ein Root-Passwort erforderlich. In Arbeitsblatt für die Kundenkonfiguration finden Sie die entsprechenden Werte.

Konfigurieren des vSphere-Netzwerks

Der *VMware vSphere-Netzwerkleitfaden* beschreibt die vSphere-Netzwerkkonfiguration, einschließlich Lastenausgleich, Linkzusammenfassung und Failover-Optionen. Wählen Sie die entsprechende Option für den Lastenausgleich auf der Basis dessen aus, was von der Netzwerkinfrastruktur unterstützt wird. Weitere Informationen finden Sie in den in Referenzdokumentation aufgeführten Dokumenten.

Netzwerkschnittstellenkarten

Während der Installation von vSphere wird ein virtueller Standard-Switch (vSwitch) erstellt. Standardmäßig wählt vSphere nur eine physische NIC als virtuellen Switch Uplink aus. Zum Erfüllen der Redundanz- und Bandbreitenanforderungen konfigurieren Sie eine zusätzliche NIC, entweder über die vSphere-Konsole oder durch eine Verbindung mit dem vSphere-Host vom vSphere-Client aus.

Jeder vSphere-Server sollte über mehrere Schnittstellenkarten für jedes virtuelle Netzwerk verfügen, um Redundanz und die Verwendung von Netzwerklastenausgleich, Linkzusammenfassung und Netzwerkadapter-Failover zu ermöglichen.

VMKernel-Ports

Erstellen Sie basierend auf der Infrastrukturkonfiguration die folgenden VMkernel-Ports nach Bedarf:

- VMkernel-Port für vMotion
- Virtuelle Desktop-Portgruppen (verwendet von den virtuellen Desktops für die Kommunikation im Netzwerk)

Im *VMware vSphere-Netzwerkleitfaden* wird das Verfahren für die Konfiguration dieser Einstellungen beschrieben. Weitere Informationen finden Sie in den in Referenzdokumentation aufgeführten Dokumenten.

Verbinden von vSphere-Datastores

Verbinden Sie die in Vorbereiten und Konfigurieren der Speicherarrays konfigurierten Datastores mit den entsprechenden vSphere-Servern. Dazu zählen die Datastores, die für die folgenden Zwecke konfiguriert wurden:

- Virtueller Desktop-Speicher
- Virtueller Infrastrukturmaschinenspeicher (falls erforderlich)
- SQL Server-Speicher (falls erforderlich)

Damit die Server auf XtremIO-Volumes zugreifen können, konfigurieren Sie XtremIO-Initiatorgruppen und fügen Sie jeder Gruppe die entsprechenden vSphere-Hosts hinzu, indem Sie die folgenden Schritte in der XtremIO Storage Management Application ausführen:

1. Klicken Sie auf **Configuration**.
2. Klicken Sie im Bereich **Initiator Group** auf **Add**.
3. Geben Sie im Fenster **Add New Initiator Group** einen Namen im Feld **Initiator Group Name** ein und klicken Sie auf **Add**.
4. Geben Sie im Fenster **Add Initiator** einen Namen in das Feld **Initiator Name** ein und wählen Sie dann in der Liste **Initiator Port Address** den Initiatorport eines vSphere-Servers aus, der in der Zielinitiatorgruppe sein sollte. Klicken Sie auf **OK**, um zum Fenster **Add Initiator** zurückzukehren.
5. Wiederholen Sie bei Bedarf im Fenster **Add Initiator** Schritt 4, um alle Zielinitiatorports der Initiatorgruppe hinzuzufügen. Sobald alle Initiatoren hinzugefügt wurden, klicken Sie auf **Finish**.

6. Wählen Sie im Menü **Configuration** im Bereich **Volumes** die Ziel-Volumes aus, wählen Sie im Bereich **Initiator Groups** die Zielinitiatorgruppe aus, klicken Sie auf die Schaltfläche **Map All** und anschließend auf **Apply**, um den Prozess abzuschließen und den vSphere-Servern den Zugriff auf die ausgewählten Volumes zu gewähren. Wiederholen Sie bei Bedarf diese Schritte, um den verbleibenden Initiatorgruppen Zugriff auf die verbleibenden Volumes zu gewähren.
7. Führen Sie auf den vSphere-Hosts den Vorgang **Rescan for Datastores** durch, damit diesen sofort die XtremIO-Volumes angezeigt werden, auf die ihnen Zugriff gewährt wurde.
8. Wiederholen Sie diesen Prozess nach Bedarf, um für jeden vSphere-Cluster eine Initiatorgruppe zu erstellen.

Der *VMware vSphere-Speicherleitfaden* enthält Anweisungen zur Formatierung der vSphere-Datastores, sobald XtremIO-Initiatorgruppen konfiguriert wurden. Weitere Informationen finden Sie in den in Referenzdokumentation aufgeführten Dokumenten.

Optimieren von vSphere für XtremIO

Mehrere Änderungen sind erforderlich, um eine optimale Performance des XtremIO-Arrays sicherzustellen, wenn es mit vSphere verwendet wird. Diese Änderungen werden im *EMC XtremIO-Speicherarray-Benutzerhandbuch* beschrieben und umfassen Folgendes:

- Ändern Sie die vSphere-Speichergerätpfadauswahl zu **Round Robin (VMware)** für jeden vSphere-Datastore. Dies können Sie mithilfe des folgenden vSphere-PowerCLI-Befehls ausführen, indem Sie anstelle von **cluster** den Namen des vSphere-Clusters eintragen, in dem sich die Ziel-vSphere-Hosts befinden. Wiederholen Sie den Vorgang je nach Bedarf für jedes Cluster:

  ```
  Get-VMHost -location cluster | get-scsilun -luntype "disk" |
  where {$_.MultipathPolicy -ne "RoundRobin"} | Set-ScsiLun -
  MultipathPolicy "RoundRobin"
  ```

- Ändern Sie die vSphere-Einstellung **Disk.SchedQuantum** in 64 und die Einstellung **Disk.DiskMaxIOSize** in 4096. Sie können dies mit den folgenden vSphere-PowerCLI-Befehlen tun, indem Sie anstelle von **cluster** den Namen des vSphere-Clusters verwenden, in dem sich die vSphere-Zielhosts befinden. Wiederholen Sie den Vorgang je nach Bedarf für jedes Cluster:

  ```
  Get-VMhost -location cluster | Set-
  VMhostAdvancedConfiguration Disk.SchedQuantum -Value 64
  Get-VMhost -location cluster | Set-
  VMhostAdvancedConfiguration Disk.DiskMaxIOSize -Value 4096
  ```

- Ändern Sie die vSphere-Einstellung **Disk.SchedNumReqOutstanding** für jeden vSphere-Datastore in 256. Dies können Sie mithilfe des folgenden vSphere-PowerCLI-Skripts erledigen. Wiederholen Sie den Vorgang je nach Bedarf für jedes vSphere-Cluster, indem Sie im Skript **ClusterName** durch den entsprechenden Zielclusternamen ersetzen:

```
$vmhosts = get-vmhost -location ClusterName
foreach ($vmhost in $vmhosts) {
$esxcli = get-esxcli -vmhost $vmhost
$AllLUNs = get-scsilun -vmhost $vmhost | where {$_.vendor -
eq "XtremIO"}
foreach ($lun in $AllLUNs) {
$CN = $lun.canonicalname
$EsxCli.storage.core.device.set($null, $cn, $null, $null,
$null, $null, $null, 256, $on)
}
}
```

Die in diesem Abschnitt beschriebenen Einstellungen gelten nur für vSphere-Hosts, die mit EMC XtremIO-Arrays verbunden sind, und sollten nicht auf Block-Datastores angewendet werden, die auf anderen Arrays, einschließlich anderer EMC Arrays, gehostet werden. Sie können diese Einstellungen auf vSphere-Hosts anwenden, die mit NFS-Datastores sowie mit einem XtremIO-Array verbunden werden, da die Einstellungen keine Auswirkung auf die Kommunikation mit diesen NFS-Datastores haben.

Installieren und Konfigurieren der SQL Server-Datenbank

In Tabelle 16 beschreibt die Aufgaben für die Einrichtung und Konfiguration einer Microsoft SQL Server-Datenbank für die Lösung. Wenn die Aufgaben abgeschlossen sind, wird SQL Server auf einer virtuellen Maschine, einschließlich aller für vCenter, Update Manager, XenDesktop und Citrix Provisioning Services erforderlichen Datenbanken, eingerichtet.

Hinweis: EMC empfiehlt, das Betriebssystem-Volume für die virtuelle SQL Server-Maschine in den Pool der VSPEX Private Cloud zu integrieren. Die empfohlenen Werte für CPU und Arbeitsspeicher sind in Tabelle 16 aufgeführt.

Tabelle 16. Aufgaben für die SQL Server-Datenbankkonfiguration

Aufgabe	Beschreibung	Referenz
Erstellen einer virtuellen Maschine für SQL Server	Erstellen Sie eine virtuelle Maschine zum Hosten von SQL Server auf einem der vSphere-Server, der für virtuelle Infrastrukturmaschinen vorgesehen ist, und verwenden Sie den für die gemeinsame Infrastruktur bestimmten Datastore. Überprüfen Sie, ob der virtuelle Server die Hardware- und Softwareanforderungen erfüllt.	*vSphere-Administratorhandbuch für virtuelle Maschinen*
Installieren von Microsoft Windows auf der virtuellen Maschine	Installieren Sie Microsoft Windows Server 2012 R12 Standard Edition auf der virtuellen Maschine.	Installieren und Bereitstellen von Windows Server 2012 R2
Installieren von SQL Server	Installieren Sie SQL Server 2012 auf der virtuellen Maschine.	SQL Server-Installation (SQL Server 2012)

Aufgabe	Beschreibung	Referenz
Konfigurieren der Datenbank für VMware vCenter Server	Erstellen Sie die für vCenter-Server erforderliche Datenbank auf dem entsprechenden Datastore.	*Vorbereiten der vCenter Server-Datenbanken*
Konfigurieren der Datenbank für VMware Update Manager	Erstellen Sie die für Update Manager erforderliche Datenbank auf dem entsprechenden Datastore.	*Vorbereiten der Update Manager-Datenbank*
Konfigurieren der VMware vCenter-Datenbankberechtigungen	Konfigurieren Sie den Datenbankserver mit den entsprechenden Berechtigungen für vCenter.	*Vorbereiten der vCenter Server-Datenbanken*
Konfigurieren der VMware Update Manager-Datenbankberechtigungen	Konfigurieren Sie den Datenbankserver mit den entsprechenden Berechtigungen für Update Manager.	*Vorbereiten der Update Manager-Datenbank*

Bereitstellen von VMware vCenter Server

In Tabelle 17 beschreibt die Aufgaben, die abgeschlossen werden müssen, um VMware vCenter Server für die Lösung zu konfigurieren.

Hinweis: EMC empfiehlt, das Betriebssystem-Volume für die virtuelle vCenter Server-Maschine in den Pool der VSPEX Private Cloud zu integrieren. Die empfohlenen Werte für CPU und Arbeitsspeicher sind in Tabelle 12 aufgeführt.

Tabelle 17. Aufgaben für die vCenter-Konfiguration

Aufgabe	Beschreibung	Referenz
Erstellen der virtuellen vCenter-Hostmaschine	Erstellen Sie eine virtuelle Maschine für vCenter Server.	*vSphere-Administratorhandbuch für virtuelle Maschinen*
Installieren des vCenter-Gastbetriebssystems	Installieren Sie Windows Server 2012 R2 Standard Edition auf der virtuellen vCenter-Hostmaschine.	VMware vSphere-Dokumentation
Aktualisieren der virtuellen Maschine	Installieren Sie VMware Tools, aktivieren Sie die Hardwarebeschleunigung und lassen Sie den Remotezugriff auf die Konsole zu.	*vSphere-Administratorhandbuch für virtuelle Maschinen*
Erstellen von vCenter ODBC-Verbindungen	Erstellen Sie die 64-Bit vCenter und 32-Bit vCenter Update Manager ODBC-Verbindungen.	*Installations- und Einrichtungshandbuch für vSphere* *Installieren und Verwalten von VMware vSphere Update Manager*

Aufgabe	Beschreibung	Referenz
Installieren von vCenter Server	Installieren Sie die vCenter Server-Software.	*Installations- und Einrichtungshandbuch für vSphere*
Installieren von vCenter Update Manager	Installieren Sie die vCenter Update Manager-Software.	*Installieren und Verwalten von VMware vSphere Update Manager*
Erstellen Sie ein virtuelles Rechenzentrum.	Erstellen Sie ein virtuelles Rechenzentrum.	*Handbuch für vCenter Server- und Hostverwaltung*
Anwenden der vSphere-Lizenzschlüssel	Geben Sie die vSphere-Lizenzschlüssel in das vCenter-Lizenzierungsmenü ein.	*Installations- und Einrichtungshandbuch für vSphere*
Hinzufügen von vSphere-Hosts	Verbinden Sie den vCenter-Server mit den vSphere-Hosts.	*Handbuch für vCenter Server- und Hostverwaltung*
Konfigurieren von vSphere-Clustering	Erstellen Sie ein vSphere-Cluster, und verschieben Sie die vSphere-Hosts in das Cluster.	*Handbuch zur vSphere-Ressourcenverwaltung*
Installieren des vCenter Update Manager-Plug-ins	Installieren Sie das vCenter Update Manager-Plug-in von der Administrationskonsole.	*Installieren und Verwalten von VMware vSphere Update Manager*
Bereitstellen von EMC PowerPath/VE	Stellen Sie mithilfe von Update Manager das PowerPath/VE-Plug-in für alle vSphere-Hosts bereit.	*Installations- und Administrationshandbuch für PowerPath/VE für VMware vSphere*
Installieren von EMC VSI für VMware vSphere-Plug-in	Installieren Sie VSI für VMware vSphere-Plug-in auf der Administrationskonsole.	*EMC VSI für VMware vSphere: Unified Storage Management – Produktleitfaden*
EMC PowerPath Viewer installieren	Installieren Sie PowerPath Viewer auf der Administrationskonsole.	*Installations- und Administrationshandbuch für EMC PowerPath Viewer*

Installieren und Konfigurieren der XenDesktop Delivery Controller

In diesem Abschnitt finden Sie Informationen zur Einrichtung und Konfiguration der XenDesktop Delivery Controller für die Lösung. Für eine Neuinstallation von XenDesktop empfiehlt Citrix, dass Sie die folgenden Aufgaben in der in 0 gezeigten Reihenfolge durchführen:

Hinweis: EMC empfiehlt, das Betriebssystem-Volume für die virtuellen Maschinen des XenDesktop Delivery Controllers in den Pool der VSPEX Private Cloud zu integrieren. Die empfohlenen Werte für CPU und Arbeitsspeicher sind in Tabelle 12 aufgeführt.

Tabelle 18. Aufgaben für die Einrichtung der XenDesktop-Controller

Aufgabe	Beschreibung	Referenz
Erstellen von virtuellen Maschinen für XenDesktop Delivery Controller	Erstellen Sie zwei virtuelle Maschinen in vSphere Client. Diese virtuellen Maschinen werden als XenDesktop Delivery Controller verwendet.	*vSphere-Administratorhandbuch für virtuelle Maschinen*
Installieren des Gastbetriebssystems für die XenDesktop Delivery Controller	Installieren Sie das Gastbetriebssystem Windows Server 2012 R2 oder Windows Server 2012 auf den virtuellen Maschinen.	
Installieren der serverseitigen Komponenten von XenDesktop	Installieren Sie die erforderlichen XenDesktop-Serverkomponenten auf dem ersten Delivery Controller.	Citrix-Website
Installieren von Citrix Studio	Installieren Sie Citrix Studio für das Remotemanagement der XenDesktop-Bereitstellung.	
Konfigurieren eines Standorts	Konfigurieren Sie einen Standort in Citrix Studio.	
Hinzufügen eines zweiten XenDesktop Delivery Controllers	Installieren Sie einen zusätzlichen Delivery Controller für hohe Verfügbarkeit.	
Vorbereiten einer virtuellen Master-Maschine	Erstellen Sie eine virtuelle Master-Maschine als Basis-Image für die virtuellen Desktops.	
Provisioning der virtuellen Desktops	Stellen Sie die virtuellen Desktops über MCS bereit.	

Installieren der serverseitigen Komponenten von XenDesktop

Installieren Sie die folgenden serverseitigen XenDesktop-Komponenten auf dem ersten Delivery Controller:

- **Delivery Controller**: Verteilt Anwendungen und Desktops, verwaltet den Benutzerzugriff und optimiert Verbindungen
- **Citrix Studio**: Erstellt, konfiguriert und verwaltet Infrastrukturkomponenten, Anwendungen und Desktops
- **Citrix Director**: Überwacht die Performance und behebt Probleme
- **Lizenzserver**: Verwaltet Produktlizenzen
- **Citrix StoreFront**: Bietet Bereitstellungsservices für die Authentifizierung und Ressourcen für Citrix Receiver

Hinweis: Citrix unterstützt die Installation von XenDesktop-Komponenten nur über die in der Citrix-Dokumentation beschriebenen Verfahren.

Konfigurieren eines Standorts

Starten Sie Citrix Studio und konfigurieren Sie einen Standort wie folgt:

1. Lizenzieren Sie den Standort, und geben Sie an, welche Edition von XenDesktop verwendet werden soll.
2. Konfigurieren Sie die Standortdatenbank mithilfe von designierten Anmeldedaten für SQL Server.
3. Stellen Sie Informationen zu Ihrer virtuellen Infrastruktur bereit, einschließlich des vCenter SDK-Pfads, den der Controller zum Einrichten einer Verbindung mit der VMware-Infrastruktur verwendet.

Hinzufügen eines zweiten Controllers

Nachdem Sie einen Standort konfiguriert haben, können Sie einen zweiten Delivery Controller hinzufügen, um hohe Verfügbarkeit bereitzustellen. Für den zweiten Controller sind die folgenden serverseitigen XenDesktop-Komponenten erforderlich:

- Delivery Controller
- Citrix Studio
- Citrix Director
- Citrix StoreFront

Installieren Sie die Lizenzserverkomponente nicht auf dem zweiten Controller, da sie zentral auf dem ersten Controller gemanagt wird.

Installieren von Citrix Studio

Installieren Sie Citrix Studio auf den gewünschten Administratorkonsolen, um Ihre XenDesktop-Bereitstellung remote zu managen.

Vorbereiten der virtuellen Mastermaschine

Führen Sie die folgenden Schritte aus, um die virtuelle Master-Maschine vorzubereiten:

1. Installieren Sie das Windows 8.1-Gastbetriebssystem.
2. Installieren Sie die entsprechenden Integrationstools, z. B. VMware Tools.
3. Optimieren Sie die Betriebssystemeinstellungen, um zu verhindern, dass unnötige Hintergrundservices irrelevante I/O-Vorgänge generieren, die sich negativ auf die allgemeine Performance des Speicherarrays auswirken. Ausführliche Informationen finden Sie im folgenden White Paper: *Optimierungshandbuch für Citrix Windows 8.1 für die Desktopvirtualisierung*.
4. Installieren Sie den Virtual Desktop Agent.
5. Installieren Sie die Drittanbietertools oder -anwendungen wie Microsoft Office, die für Ihre Umgebung relevant sind.
6. Installieren Sie den Avamar Desktop/Laptop-Client.

Provisioning der virtuellen Desktops

Gehen Sie in Citrix Studio wie folgt vor, um MCS-basierte virtuelle Desktops bereitzustellen:

1. Erstellen Sie einen Maschinenkatalog, und verwenden Sie die virtuelle Master-Maschine als Basis-Image.

   MCS ermöglichen die Erstellung eines Maschinenkatalogs, der verschiedene Desktoptypen enthält. Für diese Lösung wurden die folgenden Desktoptypen getestet:

   - **Windows Desktop Betriebssystem**:
     - Zufällig: Benutzer verbinden sich bei jeder Anmeldung mit einem neuen (zufällig ausgewählten) Desktop.
     - PvD: Benutzer verbinden sich bei jeder Anmeldung mit demselben (statischen) Desktop. Änderungen werden auf einem separaten PvD gespeichert.
   - **Windows Server-Betriebssystem**: Stellt gehostete, gemeinsam genutzte Desktops für die Bereitstellung standardisierter Maschinen zur Verfügung

2. Fügen Sie die im Katalog erstellten Maschinen einer Bereitstellungsgruppe hinzu, damit die virtuellen Desktops für Anwender zur Verfügung stehen.

Installieren und Konfigurieren von Citrix Provisioning Services

In diesem Abschnitt finden Sie Informationen zum Einrichten und Konfigurieren von Citrix PVS für die Lösung. Für eine Neuinstallation von PVS empfiehlt Citrix, dass Sie die folgenden Aufgaben in der in Tabelle 19 gezeigten Reihenfolge durchführen:

Tabelle 19. Aufgaben für die Einrichtung der XenDesktop-Controller

Aufgabe	Beschreibung	Referenz
Erstellen von virtuellen Maschinen für PVS-Server	Erstellen Sie zwei virtuelle Maschinen in vSphere Client. Diese virtuellen Maschinen werden als PVS-Server verwendet.	*vSphere-Administrator-handbuch für virtuelle Maschinen*
Installieren des Gastbetriebssysteme für die PVS-Server	Installieren Sie das Gastbetriebssystem Windows Server 2012 R2 oder Windows Server 2012 für die PVS-Server.	
Installieren der serverseitigen PVS-Komponenten	Installieren Sie die PVS-Serverkomponenten und die Konsole auf dem PVS-Server.	Citrix-Website
Konfigurieren einer PVS-Serverfarm	Führen Sie den Provisioning Services-Konfigurationsassistenten aus, um eine PVS-Serverfarm zu erstellen.	
Hinzufügen eines zweiten PVS-Servers	Installieren Sie die PVS-Serverkomponenten und die Konsole auf dem zweiten Server und verbinden Sie diesen mit der vorhandenen Serverfarm.	

Aufgabe	Beschreibung	Referenz
Erstellen eines PVS-Speichers	Geben Sie den Speicherpfad an, in dem sich die vDisks befinden werden.	
Konfigurieren der eingehenden Kommunikation	Passen Sie die Gesamtzahl der Threads an, die für die Kommunikation mit den einzelnen virtuellen Desktops verwendet werden.	
Konfigurieren einer Bootstrap-Datei	Aktualisieren Sie das Bootstrap-Image, damit beide PVS-Server Streaming-Services bereitstellen können.	
Konfigurieren der Startoptionen 66 und 67 auf dem DHCP-Server	Geben Sie die TFTP-Server-IP und den Namen des Bootstrap-Image an, das zum Booten der Preboot eXecution Environment (PXE) verwendet wird.	
Vorbereiten einer virtuellen Master-Maschine	Erstellen Sie eine virtuelle Master-Maschine als Basis-Image für die virtuellen Desktops.	
Provisioning der virtuellen Desktops	Stellen Sie die virtuellen Desktops über PVS bereit.	

Konfigurieren einer PVS-Serverfarm

Führen Sie nach dem Installieren der PVS-Serverkomponenten den Provisioning Services-Konfigurationsassistenten aus, und konfigurieren Sie wie folgt eine neue Serverfarm:

1. Geben Sie den DHCP-Service an, der auf einem anderen Computer ausgeführt werden soll.
2. Geben Sie den PXE-Service an, der auf diesem Computer ausgeführt werden soll.
3. Wählen Sie **Create farm** aus, um eine neue PVS-Serverfarm mittels einer für diesen Zweck vorgesehenen SQL Server-Datenbankinstanz zu erstellen.
4. Wenn Sie eine neue Serverfarm erstellen, müssen Sie auch einen Standort erstellen. Vergeben Sie für den neuen Standort und die Zielgerätesammlung geeignete Namen.
5. Wählen Sie den Lizenzserver aus, der auf dem XenDesktop-Controller ausgeführt wird.
6. Wählen Sie die Option **Use the Provisioning Services TFTP service** aus.

Hinzufügen eines zweiten PVS-Servers

Nachdem Sie eine zweite PVS-Serverfarm konfiguriert haben, können Sie einen zweiten PVS-Server hinzufügen, um hohe Verfügbarkeit bereitzustellen. Installieren Sie die PVS-Serverkomponenten und die Konsole auf dem zweiten Server, und führen Sie den Provisioning Services-Konfigurationsassistenten aus, um den zweiten Server mit der bestehenden Serverfarm zu verbinden.

Erstellen eines PVS-Speichers

Ein PVS-Speicher ist ein logischer Container für vDisks. Bei der Bereitstellung von PVS-Servern in Datastores, die sich in einem XtremIO-Array befinden, müssen die PVS-Speicher mithilfe von virtuellen Laufwerken konfiguriert werden, die jedem PVS-Server zugewiesen sind.

Konfigurieren der eingehenden Kommunikation

Jeder PVS-Server verfügt über eine Reihe von User Datagram Protocol (UDP)-Ports, um die gesamte eingehende Kommunikation der virtuellen Desktops zu verwalten. Im Idealfall sollte für jede Desktopsitzung ein dedizierter Thread zur Verfügung stehen. Die Gesamtzahl der von einem PVS-Server unterstützten Threads wird wie folgt berechnet:

```
Gesamt-Threads = (Anzahl der UDP-Ports * Threads pro Port *
Anzahl der Netzwerkadapter)
```

Passen Sie die Thread-Zahl entsprechend an die Anzahl der bereitgestellten virtuellen Desktops an.

Konfigurieren einer Bootstrap-Datei

Gehen Sie zum Aktualisieren der Bootstrap-Datei, die für den PXE-Boot der virtuellen Desktops erforderlich sind, wie folgt vor:

1. Wählen Sie in der Provisioning Services-Konsole **Farm › Sites › Site-name › Servers** aus.
2. Klicken Sie mit der rechten Maustaste auf einen Server, und wählen Sie **Configure Bootstrap** aus.

   Das Dialogfeld **Configure Bootstrap** wird angezeigt, wie in Abbildung 12 gezeigt.

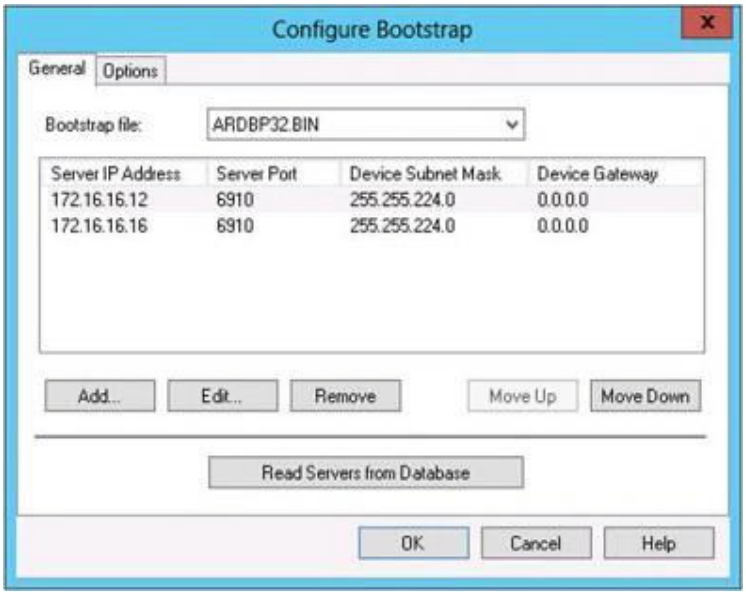

Abbildung 12. Dialogfeld Configure Bootstrap

3. Aktualisieren Sie das Bootstrap-Image zum Abbilden der IP-Adressen, die für alle PVS-Server verwendet werden, die Streaming-Services nach dem Rotationsprinzip ermöglichen. Wählen Sie **Read Servers from Database** aus, um automatisch eine Liste der PVS-Server zu erhalten, oder wählen Sie **Add** aus, um die Serverinformationen manuell hinzuzufügen.
4. Wenn Sie die Konfiguration eingestellt haben, klicken Sie auf **OK**, um die Bootstrap-Datei ARDBP32.BIN zu aktualisieren, die sich im Verzeichnis C:\ProgramData\Citrix\Provisioning Services\Tftpboot befindet.
5. Navigieren Sie zu dem Ordner, und prüfen Sie den Zeitstempel der Bootstrap-Datei, um sicherzustellen, dass sie auf dem gewünschten PVS-Server aktualisiert wird.

Konfigurieren der Startoptionen 66 und 67 auf dem DHCP-Server

Um für die virtuellen Desktops einen PXE-Boot aus dem von den PVS-Servern bereitgestellten Bootstrap-Image durchzuführen, legen Sie auf dem Microsoft DHCP-Server die Startoptionen 66 und 67 fest.

Führen Sie die folgenden Schritte aus, um die Startoptionen auf dem DHCP-Server zu konfigurieren:

1. Klicken Sie auf der DHCP-Managementoberfläche des DHCP-Servers mit der rechten Maustaste auf **Scope Options** und wählen Sie anschließend **Configure Options** aus.
2. Wählen Sie **066 Boot Server Host Name** aus. Geben Sie im Feld **String Value** die IP-Adresse des als TFTP-Server konfigurierten PVS-Servers ein.
3. Wählen Sie **067 Bootfile Name** aus. Geben Sie im Feld **String value** den Wert **„ARDBP32.BIN“** ein.

   Das Bootstrap-Image ARDBP32.BIN wird auf einen virtuellen Desktop geladen, bevor das vDisk-Image von den PVS-Servern gestreamt wird.

Vorbereiten der virtuellen Mastermaschine

Führen Sie die folgenden Schritte aus, um die virtuelle Master-Maschine vorzubereiten:

1. Installieren Sie das Windows 8.1-Gastbetriebssystem.
2. Installieren Sie entsprechende Integrationstools wie VMware Tools.
3. Optimieren Sie die Betriebssystemeinstellungen, um zu verhindern, dass unnötige Hintergrundservices irrelevante I/O-Vorgänge generieren, die sich negativ auf die allgemeine Performance des Speicherarrays auswirken. Ausführliche Informationen finden Sie im folgenden White Paper: *Optimierungshandbuch für Citrix Windows 8.1 für die Desktopvirtualisierung*.
4. Installieren Sie den Virtual Desktop Agent.
5. Installieren Sie die Drittanbietertools oder -anwendungen wie Microsoft Office, die für Ihre Umgebung relevant sind.
6. Installieren Sie die Software für das PVS-Zielgerät auf der virtuellen Master-Maschine.
7. Ändern Sie das BIOS der virtuellen Master-Maschine so, dass der Netzwerkadapter ganz oben im Boot-Auftrag steht, um den PXE-Boot des PVS-Bootstrap-Images sicherzustellen.

Provisioning der virtuellen Desktops

Gehen Sie wie folgt vor, um die PVS-basierten virtuellen Desktops bereitzustellen:

1. Führen Sie den Assistenten für das PVS-Imaging aus, um ein Clone des Masterimages auf einem vDisk zu erstellen.
2. Wenn der Clone-Vorgang abgeschlossen ist, fahren Sie die virtuelle Mastermaschine herunter, und ändern Sie die folgenden vDisk-Eigenschaften:
   - **Zugriffsmodus**: Standardimage
   - **Cachetyp**: Cache auf dem Gerätelaufwerk
3. Bereiten Sie eine Vorlage für eine virtuelle Maschine vor, die der XenDesktop-Installationsassistent im nächsten Schritt verwenden kann.

4. Führen Sie den XenDesktop-Installationsassistenten in der PVS-Konsole aus, um einen Maschinenkatalog zu erstellen, der die festgelegte Anzahl der virtuellen Desktops enthält.
5. Fügen Sie die im Katalog erstellten virtuellen Desktops einer Bereitstellungsgruppe hinzu, damit die virtuellen Desktops für Anwender zur Verfügung stehen.

Einrichten von EMC Avamar

Übersicht über die Avamar-Konfiguration

In diesem Abschnitt finden Sie Informationen zur Installation und Konfiguration von Avamar zur Unterstützung von Guest-basierten Backups von Benutzerdateien. Zwar gibt es auch andere Avamar-basierte Methoden für das Backup von Benutzerdateien, Guest-basierte Backups stellen jedoch Funktionen für die Wiederherstellung durch den Anwender über eine gemeinsame grafische Benutzeroberfläche bereit. Für diese Konfiguration wird davon ausgegangen, dass nur die Dateien und das Profil von Benutzern gesichert werden.

In Tabelle 20 sind die Aufgaben beschrieben, die abgeschlossen werden müssen.

Hinweis: Die von dem hier beschriebenen Verfahren erstellten Backups sollten durch regelmäßige Backups der Komponenten der Rechenzentrumsinfrastruktur ergänzt werden, die für virtuelle XenDesktop-Desktops erforderlich sind. Für eine vollständige Disaster Recovery müssen sowohl die Daten von XenDesktop-Endbenutzern als auch über Citrix XenDesktop bereitgestellte virtuelle Desktopbenutzerdaten und -dateien wiederhergestellt werden können.

Tabelle 20. Aufgaben für die Avamar-Integration

Aufgabe	Beschreibung	Referenz
Vorbereitung von Microsoft Active Directory		
Konfigurieren von GPO-Ergänzungen (Group Policy Object) für Avamar	Erstellen und konfigurieren Sie das GPO, um Avamar-Backups von Benutzerdateien und -profilen zu aktivieren.	*Administratorhandbuch für EMC Avamar 7*
Vorbereiten des Master Image (Goldimage) für Citrix XenDesktop		
Vorbereiten des Master-Image für Avamar	Installieren und konfigurieren Sie den Avamar Client so, dass er im Benutzermodus ausgeführt wird.	• Installieren und Konfigurieren der XenDesktop Delivery Controller • Vorbereiten der virtuellen Mastermaschine

Aufgabe	Beschreibung	Referenz
Vorbereiten von Avamar		
Definieren von Avamar-Datasets	Erstellen und konfigurieren Sie Avamar Datasets zur Unterstützung von Benutzerdateien und -profilen.	• *Administratorhandbuch für EMC Avamar 7* • *Betriebliche Best Practices für EMC Avamar 7*
Definieren von Avamar-Backupplänen	Erstellen und konfigurieren Sie einen Avamar-Backupplan, um Backups der virtuellen Desktops zu unterstützen.	
Anpassen der Wartungs-fensterplanung	Ändern Sie die Wartungszeitfensterplanung, um Backups der virtuellen Desktops zu unterstützen.	
Definieren von Avamar-Aufbewahrungs-Policies	Erstellen und konfigurieren Sie die Avamar-Aufbewahrungs-Policy.	
Erstellen einer Avamar-Gruppe und Gruppen-Policy	Erstellen und konfigurieren Sie die Avamar-Gruppe und Gruppen-Policy.	
Nach der Desktopbereitstellung		
Aktivieren von XenDesktop-Clients (Desktops)	Aktivieren Sie über Citrix XenDesktop bereitgestellte virtuelle Desktops mithilfe von Avamar Enterprise Manager.	*Administratorhandbuch für EMC Avamar 7*

Konfigurieren von GPO-Ergänzungen (Group Policy Object) für Avamar

Aufgrund von aktuellen Avamar-Einschränkungen (fehlender Support für clientseitige Variablen, z. B. **%username%**) und zur Reduzierung des Managementaufwands müssen Sie zugeordnete Laufwerke für Benutzerdaten und Benutzerprofile verwenden.

Um die zugeordneten Laufwerke zu erstellen und die Windows-Ordnerumleitung zur Erstellung der für die Laufwerke erforderlichen UNC-Pfade (Universal Naming Convention) zu konfigurieren, erstellen und bearbeiten Sie ein neues GPO im Gruppenrichtlinienverwaltungs-Editor, wie in den folgenden Verfahren beschrieben.

Ordnerumleitung

So konfigurieren Sie die Windows-Ordnerumleitung:

1. Navigieren Sie zur Policy-Einstellung **User Configuration › Policies › Windows Settings › Folder Redirection**.
2. Klicken Sie mit der rechten Maustaste auf **Documents**.
3. Wählen Sie **Properties**.
4. Wählen Sie im Listenfeld **Settings** die Option **Basic – Redirect everyone's folder to the same location** aus.
5. Geben Sie **\\CIFS_server\folder**, wie in Abbildung 13 gezeigt, ein.

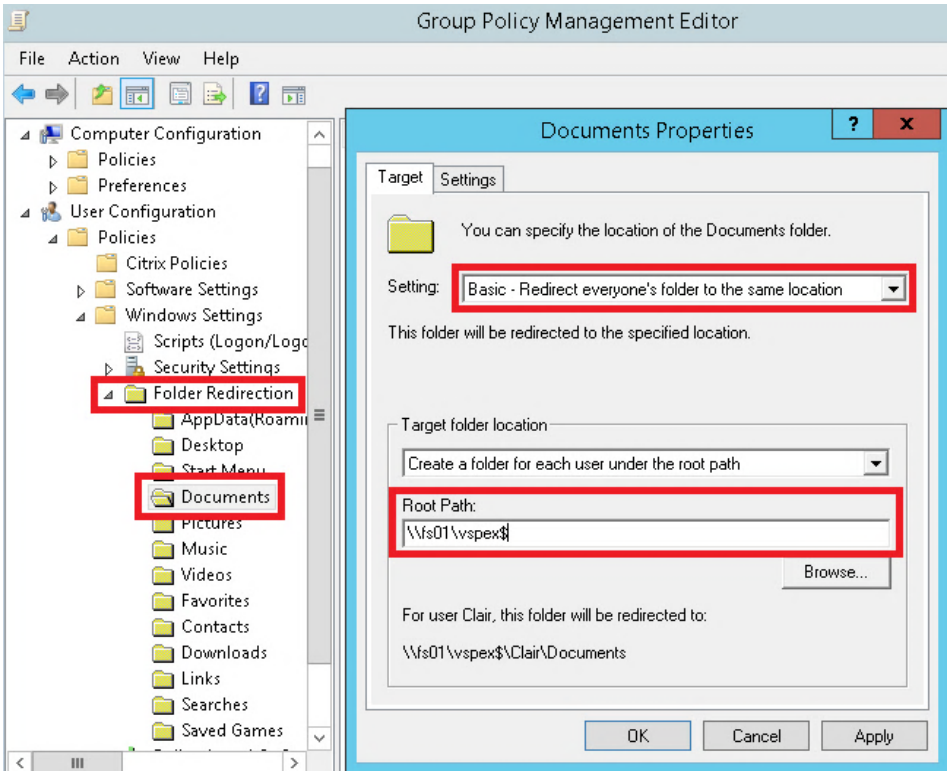

Abbildung 13. Konfigurieren der Windows-Ordnerumleitung

Zugeordnete Laufwerke

Erstellen Sie zwei zugeordnete Laufwerkskonfigurationen, eine für Benutzerdateien, die andere für Benutzerprofile. Gehen Sie für jedes zugeordnete Laufwerk gleich vor, verwenden Sie dabei aber unterschiedliche Werte für **Location**, **Label As** und **Drive Letter Used**.

So konfigurieren Sie Laufwerkszuordnungen:

1. Navigieren Sie zur Policy-Einstellung **User Configuration › Preferences › Windows Settings › Drive Maps** .
2. Klicken Sie mit der rechten Maustaste in den leeren (weißen) Bereich auf der rechten Seite des Fensters.
3. Wählen Sie **New › Mapped Drive** aus, wie in Abbildung 14 gezeigt.

   Das Fenster mit den Eigenschaften des zugeordneten Laufwerks wird angezeigt.

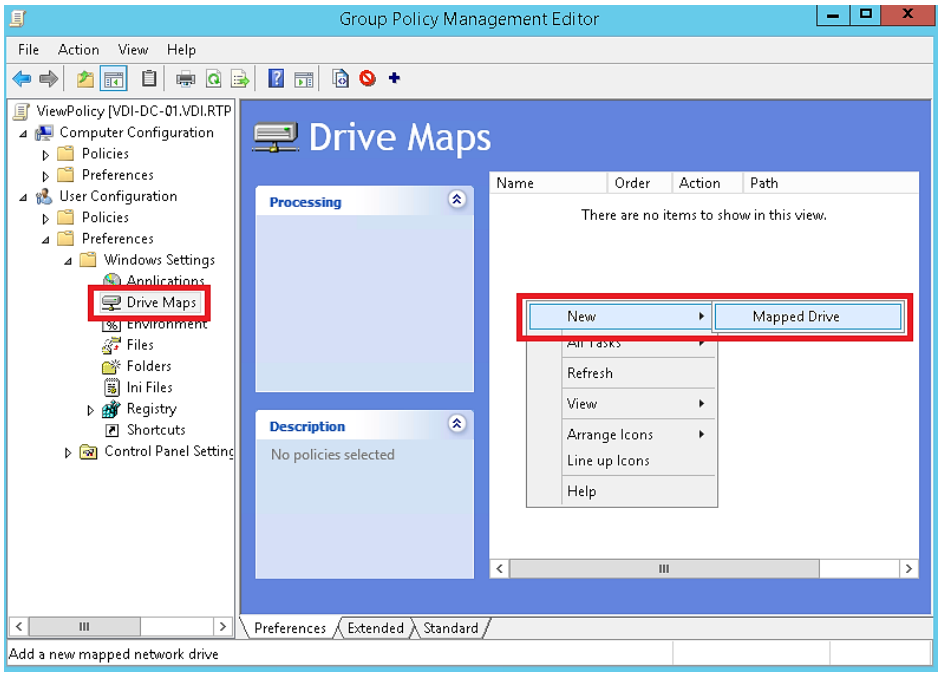

Abbildung 14. Öffnen des Dialogfelds Mapped Drive Properties

4. Führen Sie die nachfolgenden Schritte aus, um das den Benutzerdateien zugeordnete Laufwerk zu erstellen, wie in Abbildung 15 gezeigt:
   a. Wählen Sie in der Liste **Action** die Option **Create** aus.
   b. Geben Sie unter **Location** den Pfad **\\cifs_server\folder\%username%** ein.
   c. Wählen Sie **Reconnect** aus.
   d. Geben Sie unter **Label as** die Zeichenfolge **User_Files** ein.
   e. Wählen Sie unter **Drive Letter** die Optionen **Use:** und **U** aus.
   f. Wählen Sie unter **Hide/Show this drive** die Option **Hide this drive** aus.

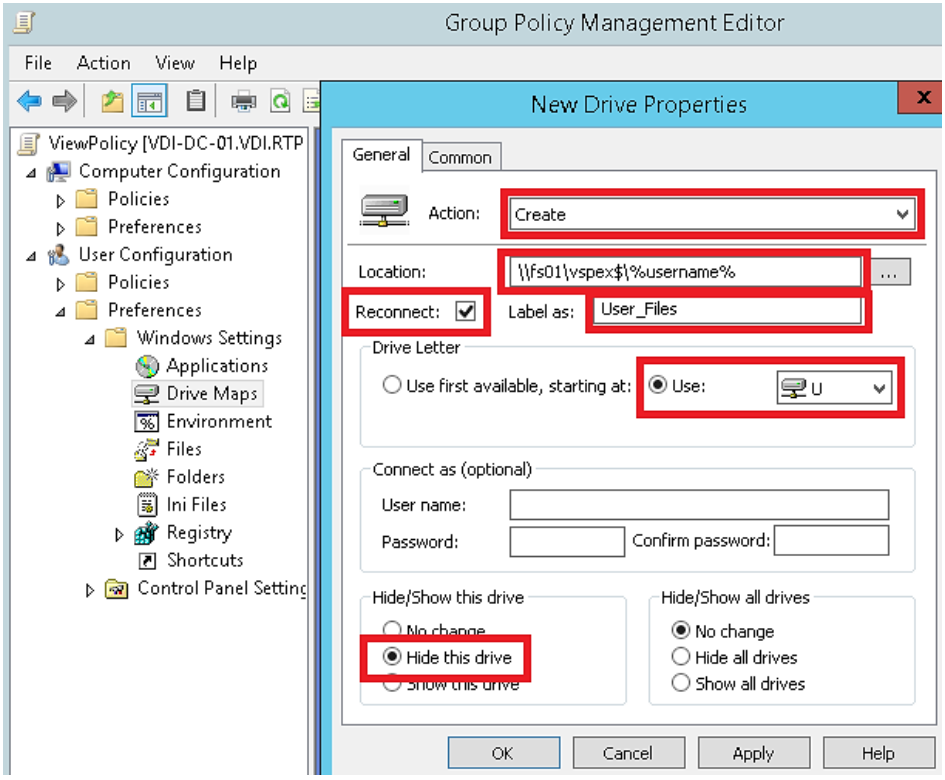

Abbildung 15. Erstellen einer Windows-Netzwerklaufwerkzuordnung für Benutzerdateien

5. Klicken Sie im Fenster **New Drive Properties** auf **Common** und wählen Sie **Run in logged-on user's security context (user policy option)** aus, wie in Abbildung 16 gezeigt.

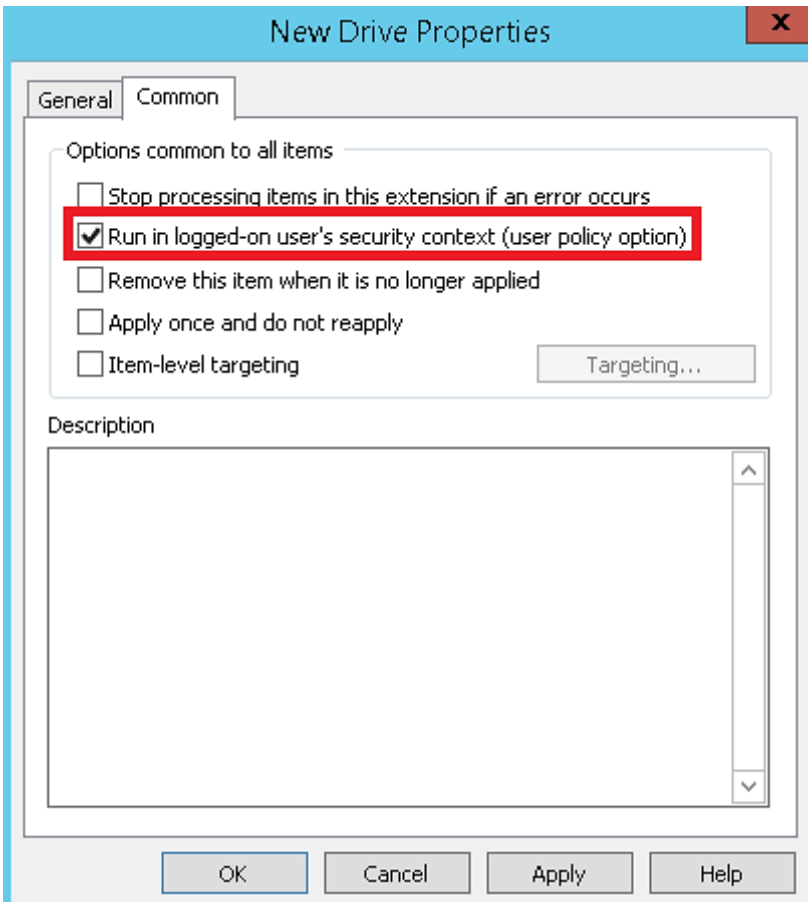

Abbildung 16. Konfigurieren der gemeinsamen Einstellungen für die Laufwerkszuordnung

6. Klicken Sie auf **Apply**.
7. So erstellen Sie das zugeordnete Laufwerk für die Benutzerprofile:
   a. Wiederholen Sie die Schritte für die Erstellung des zugeordneten Laufwerks für Benutzerdateien. Ändern Sie jedoch die folgenden drei Variablen wie angegeben (in Abbildung 17 wird eine Beispielkonfiguration gezeigt):
      - Geben Sie unter **Location** den Pfad **\\cifs_server\folder\%username%.domain.V2** ein, wobei „domain“ für den Active Directory-Domainnamen steht.
      - Geben Sie unter **Label as** die Zeichenfolge **User_Profile** ein.
      - Wählen Sie unter **Drive Letter** die Optionen **Use:** und **P** aus.

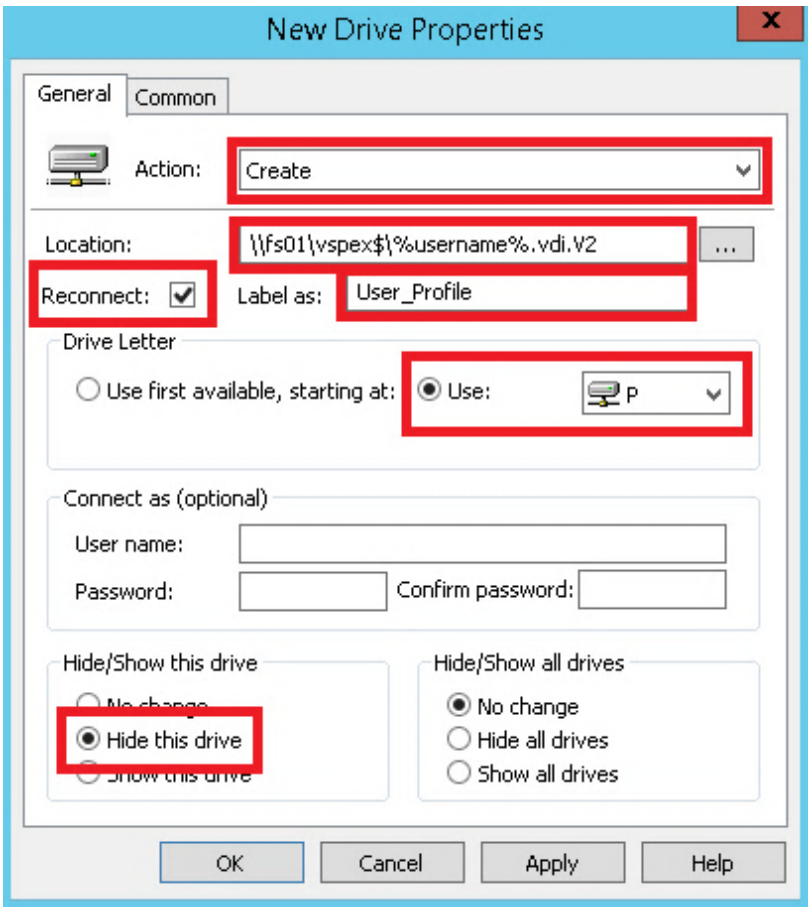

Abbildung 17. Erstellen einer Windows-Netzwerklaufwerkzuordnung für Benutzerprofildaten

8. Klicken Sie auf **OK**.
9. Schließen Sie das Fenster **Group Policy Management Editor**.

Windows-Sicherheit für den Avamar Client-Service

In diesem Abschnitt finden Sie Informationen zur Verwendung von Avamar Client für Windows zur Bereitstellung von Datensicherheit für virtuelle XenDesktop-Desktops, auf denen von Benutzern generierte Dateien in VNX-Stammverzeichnissen gespeichert werden.

Avamar Client für Windows wird als Windows-Service namens „Backup Agent“ installiert und ausgeführt. Dieser Service stellt Backup- und Wiederherstellungsfunktionen bereit.

Die Windows-Sicherheit schränkt den Zugriff von Services, die über das lokale Systemkonto angemeldet sind, auf lokale Ressourcen ein. In der Standardkonfiguration verwendet der Backup-Agent das lokale Systemkonto zur Anmeldung. Der Agent kann nicht auf Netzwerkressourcen zugreifen, einschließlich des XenDesktop-Benutzerprofils und der Datendateifreigaben.

Um auf XenDesktop-Shares mit dem Profil und den Datendateien des Benutzers zugreifen zu können, muss der Backup-Agent als derzeit angemeldeter Benutzer ausgeführt werden. Eine Batchdatei startet den Backup-Agent und meldet ihn als Benutzer an, wenn sich der Benutzer anmeldet.

Definieren von Avamar-Datasets

In den nächsten Abschnitten wird davon ausgegangen, dass Avamar Grid betriebsbereit ist und ordnungsgemäß funktioniert und Sie sich bei Avamar Administrator angemeldet haben. Weitere Informationen zum Zugriff auf Avamar Administrator finden Sie im *Administrationshandbuch für EMC Avamar 7*.

Ein Avamar-Dataset besteht aus Listen mit Verzeichnissen und Dateien, die von einem Client gesichert werden sollen. Wenn Sie einem Client oder einer Gruppe ein Dataset zuweisen, ersparen Sie sich die Backup-Auswahl. Zusätzliche Informationen zu Datasets finden Sie im *Administrationshandbuch für EMC Avamar 7*.

In diesem Abschnitt finden Sie spezifische Informationen zur Dataset-Konfiguration für virtuelle XenDesktop-Desktops, die für erfolgreiche Backups von Benutzerdateien und Benutzerprofilen erforderlich sind. Erstellen Sie zwei Datasets, eines für Benutzerdateien, das andere für Benutzerprofile. Gehen Sie für jedes Dataset gleich vor, verwenden Sie jedoch unterschiedliche Werte für **Name** und **Drive Letter Used**. Es gibt außerdem zusätzliche Schritte für die Erstellung des Benutzerprofil-Datasets.

1. Klicken Sie im Avamar Administrator-Fenster, das in Abbildung 18 dargestellt ist, auf **Tools** und wählen Sie **Manage Datasets** aus.

Abbildung 18. Konfigurieren der Windows-Ordnerumleitung

2. Klicken Sie im Fenster **Manage All Datasets** auf **New**.
3. Wählen Sie im Fenster **New Dataset** die in Abbildung 19 gezeigten benutzerdefinierten Einstellungen aus.

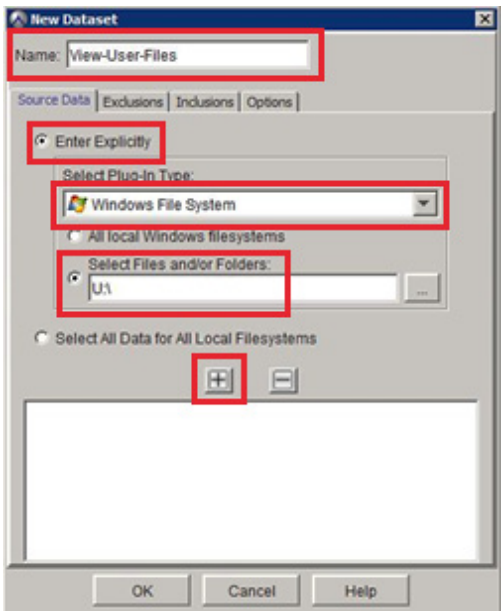

Abbildung 19. Konfigurieren der Einstellungen für das Avamar-Dataset

a. Entfernen Sie alle anderen Plug-ins aus der Liste, indem Sie jedes einzeln auswählen und auf die Schaltfläche zum Entfernen (**–**) klicken.

b. Geben Sie im Feld **Name** die Zeichenfolge **View-User-Files** ein.

c. Wählen Sie **Enter Explicitly** aus.

d. Wählen Sie im Listenfeld **Select Plug-In Type** den Eintrag **Windows File System** aus.

e. Geben Sie unter **Select Files and/or Folders „U:\“** ein und klicken Sie auf die Schaltfläche zum Hinzufügen (**+**).

4. Klicken Sie auf **OK**, um das Dataset zu speichern.

5. Wiederholen Sie die Schritte 1 bis 4 und verwenden Sie die folgenden Werte, um ein neues Dataset für Benutzerprofildaten zu erstellen:

   - Geben Sie unter **Name „View-User-Profile“** ein.
   - Geben Sie unter **Select Files and/or Folders** die Zeichenfolge **P:** ein.

   Für das Backup von **User Profile**-Daten sind zusätzliche Konfigurationseinstellungen erforderlich. In Abbildung 20 finden Sie eine Beispielkonfiguration.

6. Klicken Sie auf **Exclusions**.

7. Wählen Sie im Listenfeld **Select Plug-In Type** den Eintrag **Windows File System** aus.

8. Geben Sie unter **Select Files and/or Folders „P:\avs“** ein und klicken Sie auf die Schaltfläche zum Hinzufügen (**+**).

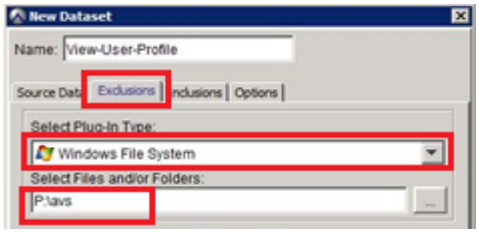

Abbildung 20. Ausschlusseinstellungen für das Benutzerprofil-Dataset

9. Klicken Sie auf **Options**, wie in Abbildung 21 gezeigt.

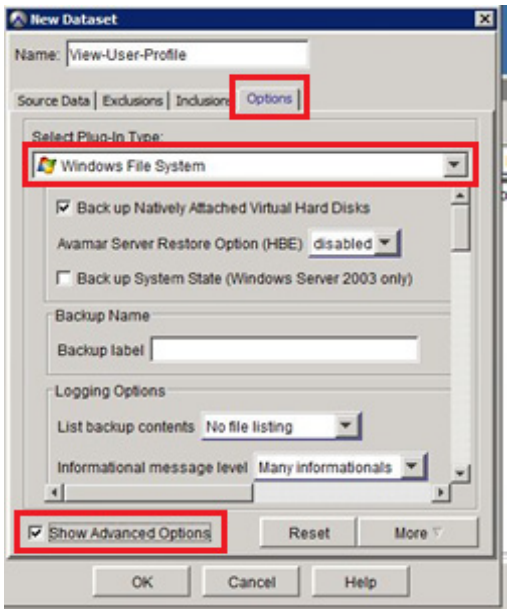

Abbildung 21. Option Select Plug-in Type

10. Wählen Sie im Listenfeld **Select Plug-In Type** den Eintrag **Windows File System** aus.
11. Wählen Sie **Show Advanced Options** aus.

12. Blättern Sie in der Liste der Optionen nach unten und wählen Sie **Volume Freezing Options** aus, wie in Abbildung 22 gezeigt.

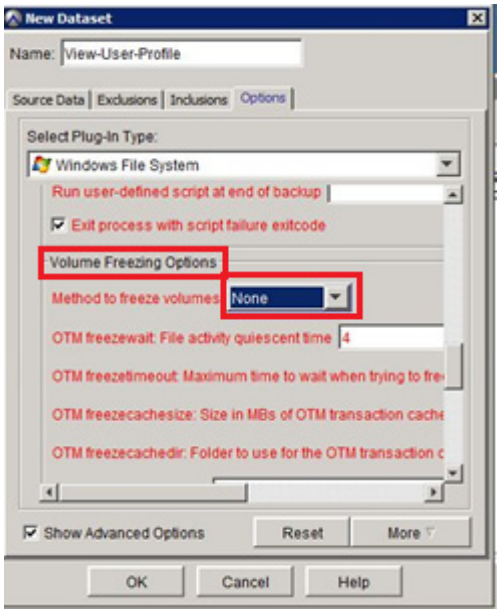

Abbildung 22. Optionen zum Sperren von Volumes

13. Wählen Sie im Listenfeld **Method to freeze volumes** die Option **None** aus.
14. Klicken Sie auf **OK**, um das Dataset zu speichern.

Definieren von Avamar-Backupplänen

Avamar-Planungen sind wiederverwendbare Objekte, die steuern, wann Gruppenbackups und benutzerdefinierte Benachrichtigungen erfolgen. Definieren Sie eine wiederkehrende Planung, die Ihren Recovery Point Objectives (RPO) entspricht. Zusätzliche Informationen zu Datasets finden Sie im *Administrationshandbuch für EMC Avamar 7*.

Anpassen der Wartungsfen-sterplanung

Die Avamar-Serverwartung umfasst die folgenden wesentlichen Aktivitäten:

- **Kontrollpunkt**: ein Snapshot des Avamar-Servers, der eigens für die Vereinfachung von Server-Rollbacks erstellt wurde.
- **Kontrollpunktvalidierung**: ein interner Vorgang, der die Integrität eines bestimmten Kontrollpunkts validiert. Wenn ein Kontrollpunkt die Validierung besteht, kann er als zuverlässig genug für ein Server-Rollback betrachtet werden.
- **Garbage Collection**: ein interner Vorgang, der Speicherplatz von gelöschten oder abgelaufenen Backups wiederherstellt.

Jeder 24-Stunden-Tag wird in drei betriebliche Zeitfenster eingeteilt, in denen verschiedene Systemaktivitäten durchgeführt werden:

- Backupzeitfenster: Der Teil jedes Tages, der zur Durchführung von normal geplanten Backups reserviert ist. Während des Backupzeitfensters werden keine Wartungsaktivitäten durchgeführt.

- Ausfallzeitfenster: Der Teil jedes Tages, der zur Durchführung von Serverwartungsaktivitäten reserviert ist, hauptsächlich die automatische Speicherbereinigung, für die unbeschränkter Zugriff auf den Server erforderlich ist. Während des Blackout-Zeitfensters sind keine Backup- oder administrativen Aktivitäten zugelassen. Wiederherstellungen sind jedoch möglich.
- Wartungszeitfenster: Der Teil jedes Tages, der für die Durchführung von Routineaktivitäten für die Serverwartung reserviert ist, hauptsächlich die Erstellung und Validierung von Kontrollpunkten.

Abbildung 23 zeigt die Avamar-Standardzeitfenster für Backup, Blackout und Wartung.

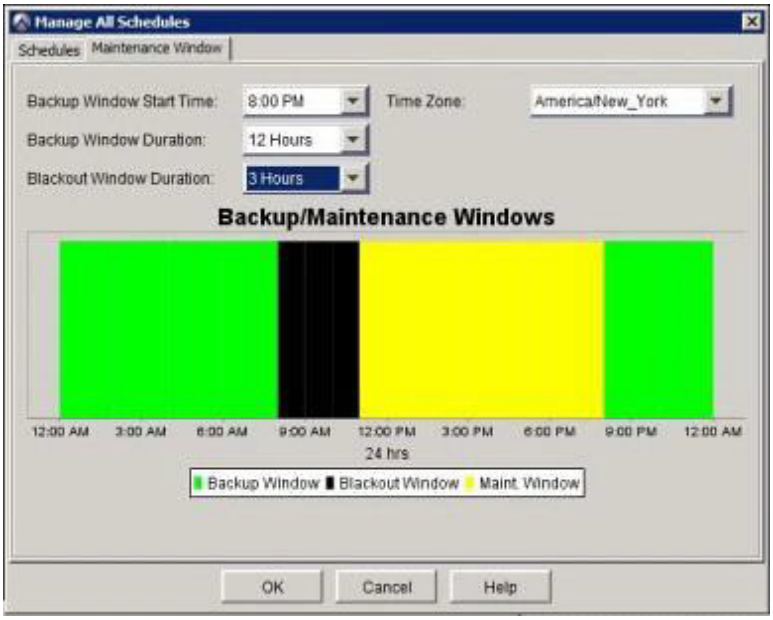

Abbildung 23. Standardplanung für Backup-/Wartungszeitfenster von Avamar

Benutzerdateien und Profildaten sollten nicht während des Tages gesichert werden, wenn Benutzer bei ihren virtuellen Desktops angemeldet sind. Passen Sie die Startzeit für das Backup-Zeitfenster an, um zu verhindern, dass in dieser Zeit Backups durchgeführt werden.

Abbildung 24 zeigt geänderte Backup-, Blackout- und Wartungszeitfenster für das Backup virtueller Citrix XenDesktop-Desktops.

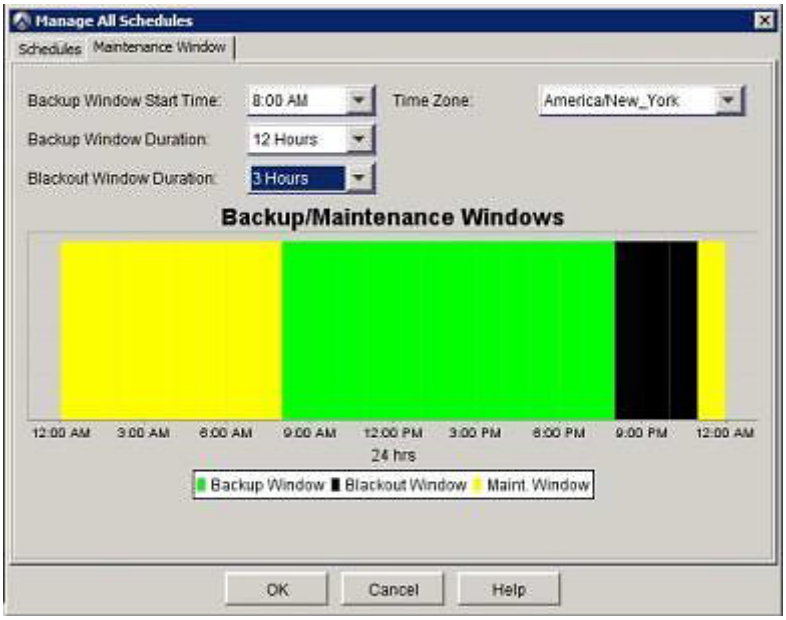

Abbildung 24. Geänderte Planung für Backup-/Wartungszeitfenster in Avamar

Damit die Planung wie oben gezeigt angepasst wird, ändern Sie die Option **Backup Window Start Time** von 20:00 in 08:00. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Zusätzliche Informationen zu Wartungsaufgaben von Avamar-Servern finden Sie im *Administrationshandbuch für EMC Avamar 7*.

Definieren von Avamar-Aufbewahrungs-Policies

Mit Avamar-Backup-Aufbewahrungs-Policies können Sie angeben, wie lange ein Backup im System aufbewahrt werden soll. Eine Aufbewahrungs-Policy wird jedem Backup während des Backup-Vorgangs zugewiesen. Geben Sie eine benutzerdefinierte Aufbewahrungs-Policy an, um ein Backup nach Bedarf durchzuführen, oder erstellen Sie eine Aufbewahrungs-Policy, die während eines geplanten Backups automatisch einer Gruppe von Clients zugewiesen wird.

Wenn die Aufbewahrung für ein Backup abgelaufen ist, wird das Backup automatisch zum Löschen gekennzeichnet. Das Löschen erfolgt in Batches zu Zeiten mit geringer Systemaktivität.

Zusätzliche Informationen zur Definition von Aufbewahrungs-Policies finden Sie im *Administrationshandbuch für EMC Avamar 7*.

Erstellen einer Avamar-Gruppe und Gruppen-Policy

Avamar verwendet Gruppen zur Implementierung verschiedener Policies für die Automatisierung von Backups sowie zur Durchsetzung konsistenter Regeln und Systemverhaltensweisen in einem gesamten Segment oder einer gesamten Gruppe der Benutzer-Community. Gruppenmitglieder sind Clientmaschinen, die für die Durchführung geplanter Backups einer bestimmten Gruppe hinzugefügt wurden.

Gruppen geben nicht nur an, welche Clients zu einer Gruppe gehören, sondern auch Folgendes:

- Datasets
- Zeitpläne
- Aufbewahrungs-Policies

Diese Objekte bilden die Gruppen-Policy, die das Backupverhalten für alle Mitglieder der Gruppe steuert, solange Sie diese Einstellungen nicht auf Clientebene außer Kraft setzen. Zusätzliche Informationen zu Gruppen und Gruppen-Policies finden Sie im *Administrationshandbuch für EMC Avamar 7*.

In diesem Abschnitt werden Informationen zur Gruppenkonfiguration bereitgestellt, die für ordnungsgemäße Backups von Benutzerdateien und Benutzerprofilen erforderlich sind.

Erstellen Sie zwei Gruppen und deren jeweilige Gruppen-Policy, eine für Benutzerdateien, die andere für Benutzerprofile. Gehen Sie für jedes Dataset gleich vor, verwenden Sie jedoch unterschiedliche Werte für **Name** und **Dataset Used**:

1. Wählen Sie in Avamar Administrator **Actions › New Group** aus, wie in Abbildung 25 gezeigt.

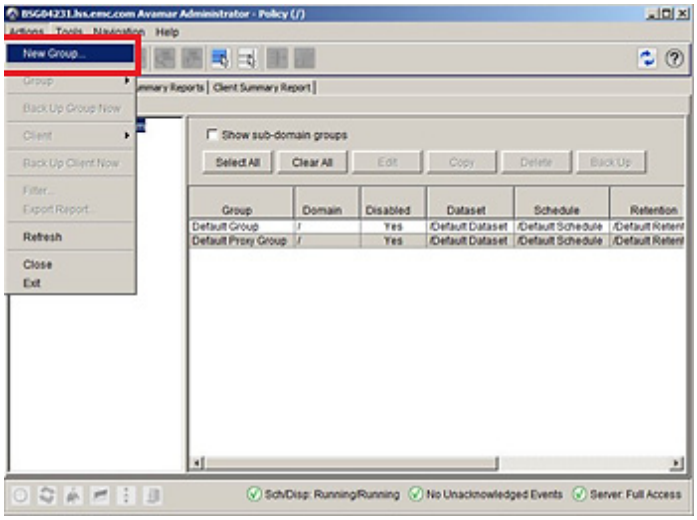

Abbildung 25. Erstellen einer neuen Avamar-Backupgruppe

Das Fenster **New Group** wird angezeigt.

2. Geben Sie unter **Name „View_User_Data“** ein, wie in Abbildung 26 gezeigt.

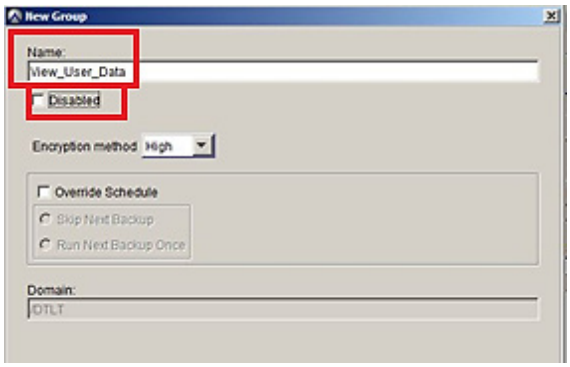

Abbildung 26. Fenster New Group

3. Vergewissern Sie sich, dass **Disabled** deaktiviert ist.
4. Klicken Sie auf **Weiter**.
5. Wählen Sie im Listenfeld **Select An Existing Dataset** die Option **Citrix Xendesktop-User-Data** aus.
6. Klicken Sie auf **Weiter**.

7. Wählen Sie im Listenfeld **Select An Existing Schedule** einen Plan aus und klicken Sie dann auf **Next**, wie in Abbildung 27 gezeigt.

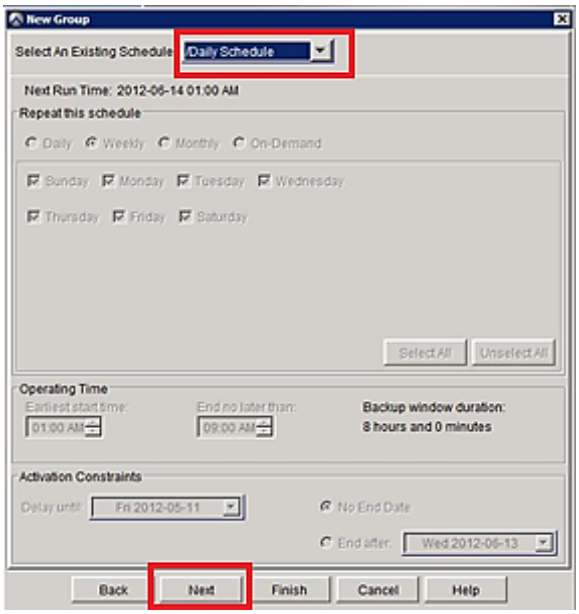

Abbildung 27. Auswählen eines vorhandenen Plans

8. Wählen Sie aus der Liste **Select An Existing Retention Policy** eine Aufbewahrungs-Policy aus.

9. Klicken Sie auf **Finish**.

Hinweis: Wenn Sie anstelle von **Finish** die Option **Next** auswählen, können Sie die Clients auswählen, die der Gruppe hinzugefügt werden sollen. Dieser Schritt ist allerdings nicht erforderlich, da Clients während der Aktivierung der Gruppe hinzugefügt werden.

Aktivieren von XenDesktop-Clients (Desktops)

Avamar Enterprise Manager ist eine webbasierte Managementkonsolenanwendung für mehrere Systeme, die zentrale Funktionen für die Avamar-Systemadministration bereitstellt, darunter die Möglichkeit, Avamar-Clients zusammengefasst hinzuzufügen und zu aktivieren.

In diesem Abschnitt wird davon ausgegangen, dass Sie wissen, wie Sie sich bei Avamar Enterprise Manager (EM) anmelden, und dass die XenDesktop-Desktops erstellt sind.

Nach der Anmeldung bei Avamar EM wird das Enterprise Manager-Dashboard angezeigt, wie in Abbildung 28 dargestellt.

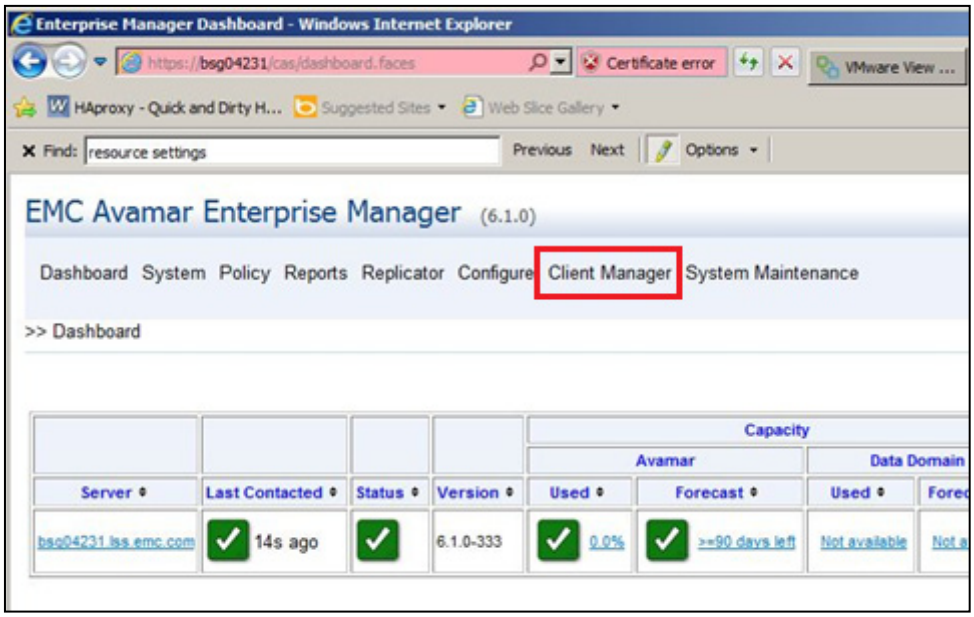

Abbildung 28. Avamar Enterprise Manager-Dashboard

1. Klicken Sie auf **Client Manager**.
2. Klicken Sie im Fenster **Avamar Client Manager** auf **Activate**, wie in Abbildung 29 gezeigt.

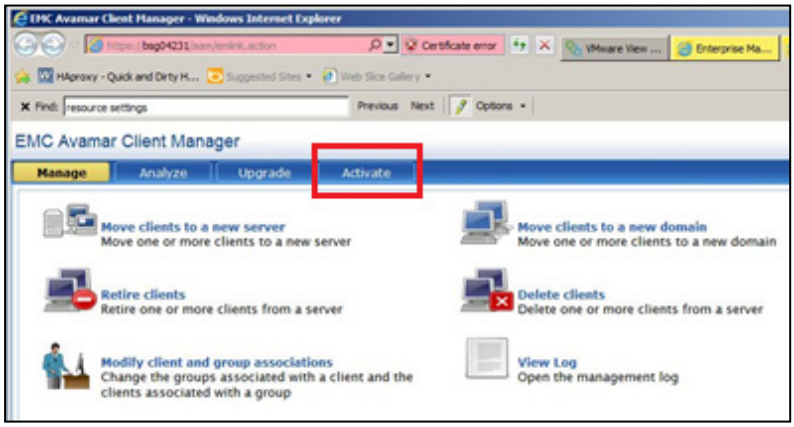
EMC Avamar Client Manager - Windows Internet Explorer
EMC Avamar Client Manager
Manage
Analyze
Upgrade
Activate
Move clients to a new server
Move one or more clients to a new server
Move clients to a new domain
Move one or more clients to a new domain
Retire clients
Retire one or more clients from a server
Delete clients
Delete one or more clients from a server
Modify client and group associations
Change the groups associated with a client and the clients associated with a group
View Log
Open the management log

Abbildung 29. Avamar Client Manager

3. Klicken Sie im Fenster **Activate** auf den Listenpfeil **Client Information** und wählen Sie **Directory Service** aus, wie in Abbildung 30 gezeigt.

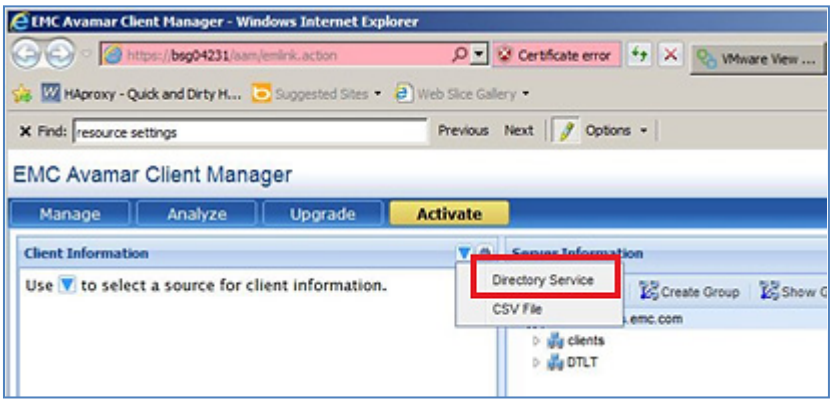

Abbildung 30. Menü mit Clientinformationen

Das Dialogfeld „Directory Service“ wird angezeigt.

4. Geben Sie die erforderlichen Benutzeranmeldedaten ein, wie in Abbildung 31 gezeigt:

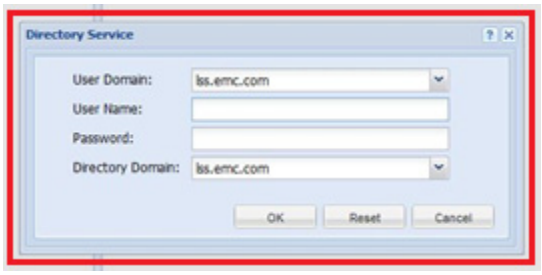

Abbildung 31. Dialogfeld Directory Service

Hierbei wird davon ausgegangen, dass ein Active Directory-Service in Avamar konfiguriert wurde. Weitere Informationen zum Aktivieren des LDAP-Managements finden Sie im *Administrationshandbuch für EMC Avamar 7.0*.

a. Wählen Sie aus der Liste **User Domain** eine Verzeichnisdienst-Domain aus.

b. Geben Sie unter **User Name** und **Password** den erforderlichen Benutzernamen und das erforderliche Passwort für die Verzeichnisdienstauthentifizierung ein.

c. Wählen Sie unter **Directory Domain** eine Verzeichnisdomain für die Abfrage von Clientinformationen aus, und klicken Sie dann auf **OK**.

Die Informationen zu Active Directory werden im Bereich **Client Information** des **Fensters EMC Avamar Client Manager** angezeigt, wie in Abbildung 32 dargestellt.

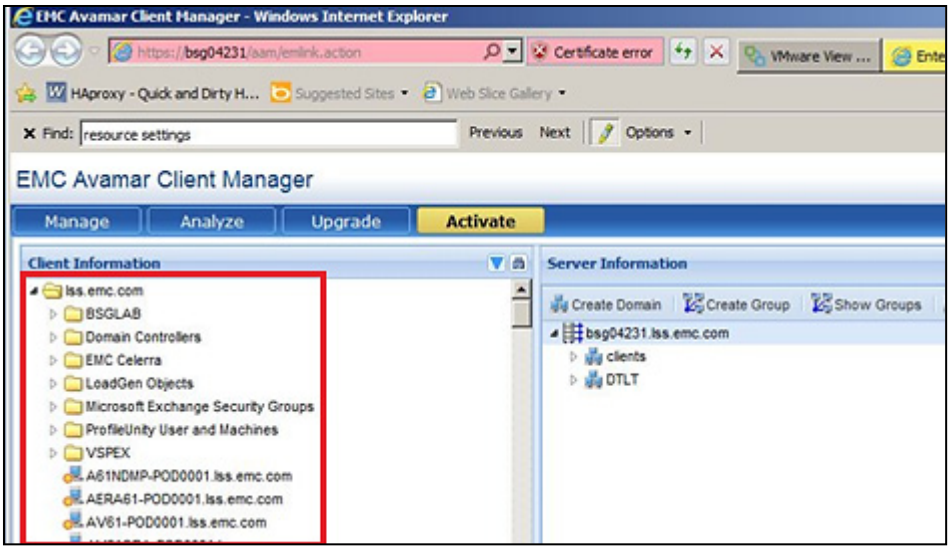

Abbildung 32. EMC Avamar Client Manager mit Active Directory-Informationen

5. Suchen Sie in der Verzeichnisstruktur **Client Information** die über **Citrix XenDesktop** bereitgestellten virtuellen Desktops aus.

   In diesem Beispiel wurde eine Organisationseinheit namens VSPEX erstellt, wie in Abbildung 33 gezeigt.

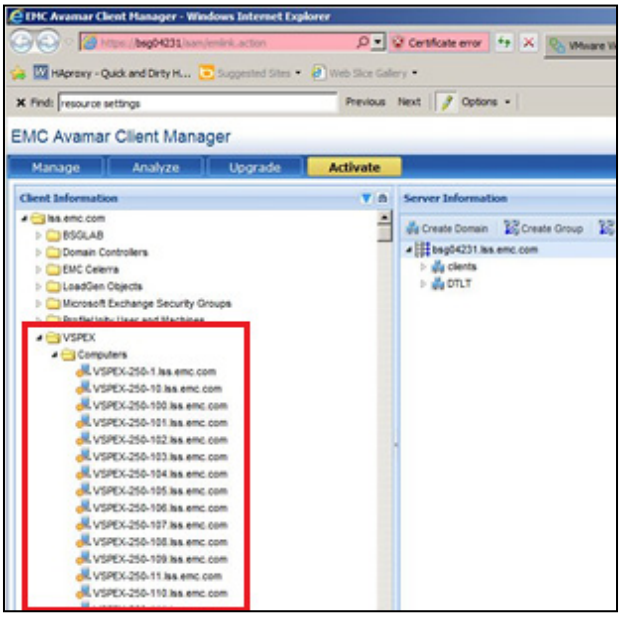

Abbildung 33. Virtuelle VSPEX-Desktops

6. Wählen Sie die virtuellen Maschinendesktops aus, die Sie zum Avamar-Server hinzufügen möchten, wie in Abbildung 34 gezeigt.

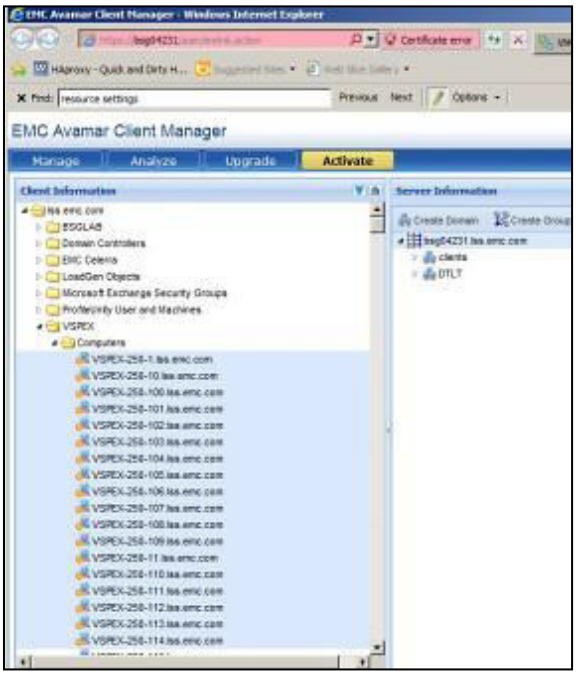

Abbildung 34. Ausgewählte virtuelle Desktops

7. Ziehen Sie die ausgewählte Liste zur vorhandenen Avamar-Domain im Fenster **Server Information**.

   Das Fenster **Select Groups** wird angezeigt, wie in Abbildung 35 dargestellt.

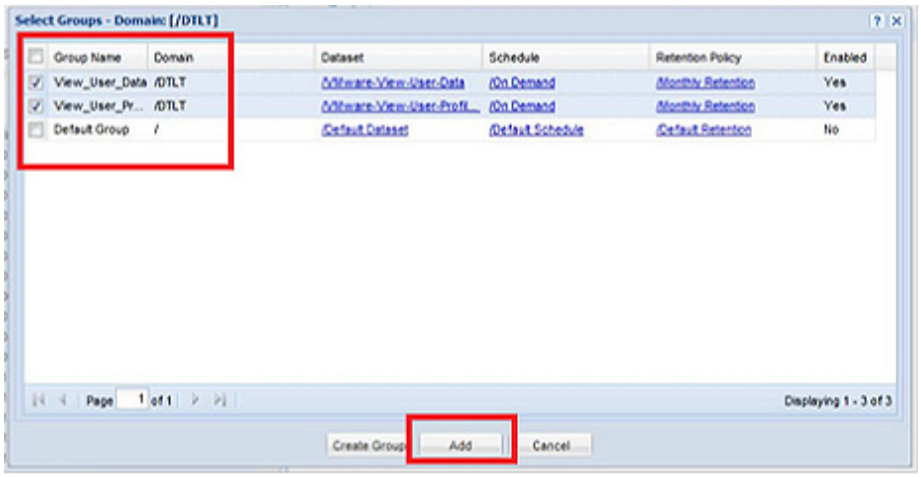

Abbildung 35. Fenster Select Groups

8. Wählen Sie unter **Group Name** die Gruppen aus, denen Sie diese Desktops hinzufügen möchten, und klicken Sie auf **Add**.

   Das Fenster **EMC Avamar Client Manager** wird erneut angezeigt.

9. Wählen Sie die Avamar-Domain aus, der Sie soeben die virtuellen Desktops hinzugefügt haben, und klicken Sie dann auf **Activate**, wie in Abbildung 36 gezeigt.

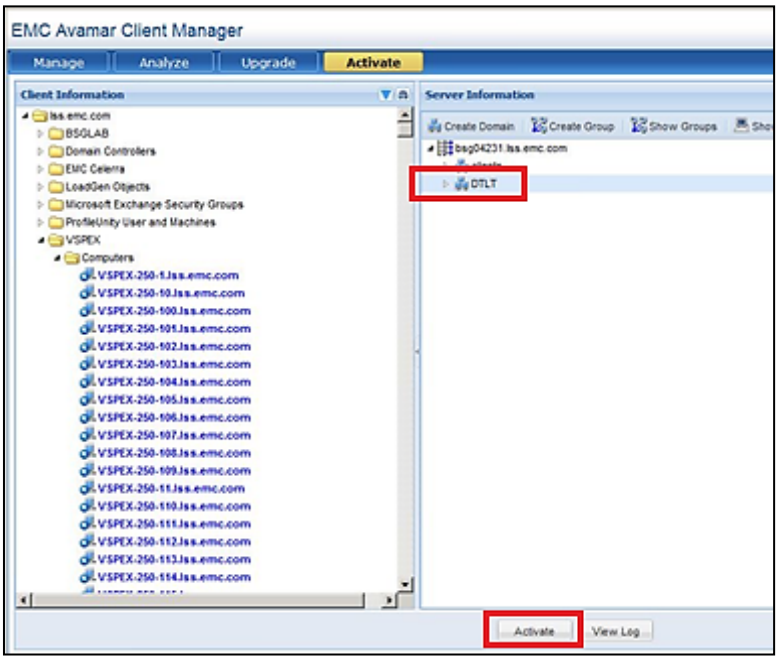

Abbildung 36. Aktivieren der Domain

Das Fenster **Show Clients for Activation** wird angezeigt.

10. Klicken Sie auf **Commit**, wie in Abbildung 37 gezeigt.

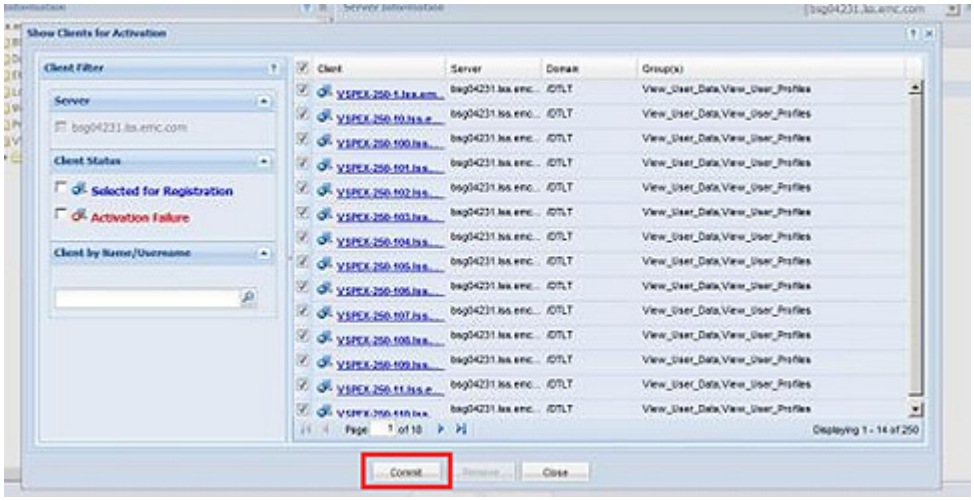

Abbildung 37. Fenster Show Clients for Activation

Es wird eine Warnmeldung angezeigt, die darauf hinweist, dass die Clientaktivierung als Hintergrundprozess durchgeführt wird.

11. Klicken Sie auf **OK**.

Eine zweite Warnmeldung weist darauf hin, dass der Aktivierungsprozess initiiert wurde und die Protokolle auf ihren Status überprüft werden sollten.

12. Klicken Sie auf **OK**.

Das Fenster **Avamar Client Manager** wird erneut mit den aktivierten Clients angezeigt, wie in Abbildung 38 dargestellt.

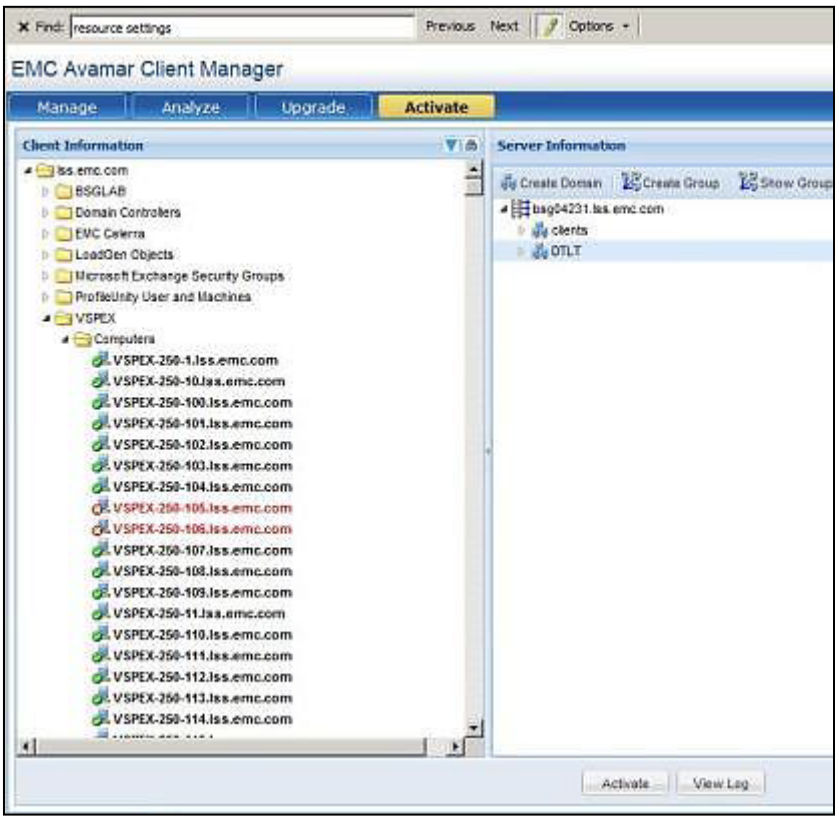

Abbildung 38. Avamar Client Manager mit aktivierten Clients

13. Melden Sie sich beim Avamar Enterprise Manager ab.

Kapitel 5 Lösungsverifizierung

In diesem Kapitel werden die folgenden Themen behandelt:

Übersicht **76**

Checkliste nach der Installation **77**

Bereitstellen und Testen eines einzelnen virtuellen Desktop **77**

Überprüfen der Redundanz der Lösungskomponenten **77**

Übersicht

Nachdem Sie die Lösung konfiguriert haben, führen Sie die Aufgaben in Tabelle 21 durch, um die Konfiguration und die Funktionen bestimmter Aspekte der Lösung zu überprüfen, und sorgen Sie dafür, dass die Konfiguration die zentralen Verfügbarkeitsanforderungen erfüllt.

Tabelle 21. Aufgaben für das Testen der Installation

Aufgabe	Beschreibung	Referenz
Überprüfen der Installation anhand der Checkliste nach der Installation.	Überprüfen Sie, ob geeignete virtuelle Ports auf jedem virtuellen vSphere-Host-Switch vorhanden sind.	*Handbuch für vSphere-Netzwerk*
	Überprüfen Sie, ob jeder vSphere-Host auf die erforderlichen Datastores und VLANs zugreifen kann.	• *Handbuch für vSphere-Speicher* • *Handbuch für vSphere-Netzwerk*
	Überprüfen Sie, ob die vMotion-Schnittstellen auf allen vSphere-Hosts korrekt installiert sind.	*Handbuch für vSphere-Netzwerk*
Bereitstellen und Testen eines einzigen virtuellen Desktops	Stellen Sie eine einzige virtuelle Maschine über die vSphere-Oberfläche bereit und nutzen Sie dabei die Anpassungsspezifikation.	• *Handbuch für vCenter Server- und Hostverwaltung* • *vSphere-Handbuch für die Verwaltung virtueller Maschinen*
Überprüfen der Redundanz der Lösungs-komponenten	Starten Sie nacheinander jeden Speicherprozessor neu und vergewissern Sie sich, dass die VMware-Datastores-Verbindung aufrechterhalten wird.	Überprüfen der Redundanz der Lösungskomponenten
	Deaktivieren Sie nacheinander jeden der redundanten Switches und überprüfen Sie, ob die Verbindung von vSphere-Host, virtueller Maschine und Speicherarray intakt bleibt.	Anbieterdokumentation
	Aktivieren Sie auf einem vSphere-Host, der mindestens eine virtuelle Maschine enthält, den Wartungsmodus und überprüfen Sie, ob die virtuelle Maschine erfolgreich zu einem alternativen Host migrieren kann.	*Handbuch für vCenter Server- und Hostverwaltung*
Provisioning der verbleibenden virtuellen Desktops	Stellen Sie Desktops über MCS oder PVS bereit.	• Installieren und Konfigurieren der XenDesktop Delivery Controller • Installieren und Konfigurieren von Citrix Provisioning Services

Checkliste nach der Installation

Die folgenden Konfigurationsaufgaben sind für die Funktionsfähigkeit der Lösung von zentraler Bedeutung. Überprüfen Sie diese, bevor Sie die Lösung in der Produktion bereitstellen. Überprüfen Sie Folgendes auf jedem vSphere-Server, der als Teil dieser Lösung verwendet wird:

- Die vSwitches, die die Client-VLANs hosten, sind mit ausreichend Ports konfiguriert, um die maximale Anzahl virtueller Maschinen zu beherbergen, die ein Host beherbergen kann.
- Alle erforderlichen virtuellen Maschinenportgruppen sind konfiguriert, und jeder Server kann auf die erforderlichen VMware-Datastores zugreifen.
- Eine Schnittstelle ist korrekt für vMotion konfiguriert. Weitere Informationen finden Sie im *VMware vSphere-Netzwerkleitfaden*.

Weitere Informationen finden Sie in den in Kapitel 6 aufgeführten Dokumenten.

Bereitstellen und Testen eines einzelnen virtuellen Desktop

Stellen Sie eine virtuelle Maschine bereit, um den Betrieb der Lösung zu überprüfen. Überprüfen Sie, ob die virtuelle Maschine der entsprechenden Domain zugeordnet ist, Zugriff auf die erwarteten Netzwerke hat und es möglich ist, sich bei ihr anzumelden.

Überprüfen der Redundanz der Lösungskomponenten

Testen Sie bestimmte Szenarios, die für die Wartung oder Hardwareausfälle relevant sind, um zu überprüfen, ob die verschiedenen Komponenten der Lösung die Verfügbarkeitsanforderungen erfüllen. Führen Sie hierzu die folgenden wichtigen Schritte aus:

1. Starten Sie nacheinander jeden XtremIO-Speicher-Controller neu und überprüfen Sie, dass die VMFS-Datastores-Verbindungen aufrechterhalten bleiben. Führen Sie die folgenden Schritte aus:
   a. Melden Sie sich über das **xinstall**-Konto beim Speicher-Controller A an.
   b. Starten Sie den Controller mithilfe der Option **6** des Installationsmenüs neu.
   c. Prüfen Sie während des Neustartzyklus das Vorhandensein von VMFS-Datastores auf den vSphere-Hosts.
   d. Überprüfen Sie mithilfe der XtremIO Storage Management Application-Benutzeroberfläche, ob Speicher-Controller A erneut online geschaltet wird, indem Sie das Warnmeldungsfenster oder die Registerkarte **Hardware** kontrollieren.
   e. Wiederholen Sie dieses Verfahren für Speicher-Controller B.

2. Starten Sie jeden VNX-Speicherprozessor nacheinander neu und überprüfen Sie, ob die Verbindungen zu den CIFS-Dateisystemen aufrechterhalten bleiben. Führen Sie die folgenden Schritte aus:
   a. Melden Sie sich mit Administratorrechten bei der Control Station an.
   b. Wechseln Sie zu **/nas/sbin**.
   c. Starten Sie SPA neu. Verwenden Sie dazu den Befehl **./navicli -h spa rebootsp**.
   d. Prüfen Sie während des Neustartzyklus das Vorhandensein von Datastores auf vSphere-Hosts.
   e. Starten Sie nach Abschluss des Zyklus SPB neu: **./navicli -h spb rebootsp**.
3. Führen Sie nacheinander ein Failover jedes VNX-Data Mover durch und überprüfen Sie, ob die Verbindungen zu den CIFS-Dateisystemen wiederhergestellt werden. Verwenden Sie den folgenden Ansatz für jeden Data Mover. Verwenden Sie die Unisphere-Benutzeroberfläche für den Neustart.
   a. Führen Sie in der $-Befehlsaufforderung der Control Station den Befehl **„server_cpu *movername*** -reboot“ aus, wobei *movername* der Name des Data Mover ist.
   b. Zum Überprüfen, ob die Netzwerkredundanzfunktionen erwartungsgemäß funktionieren, deaktivieren Sie nacheinander die redundanten Switching-Infrastrukturen. Während jede der Switching-Infrastrukturen deaktiviert ist, überprüfen Sie, ob alle Komponenten der Lösung die Verbindung miteinander und zu jeder vorhandenen Clientinfrastruktur aufrechterhalten.
4. Aktivieren Sie auf einem vSphere-Host, der mindestens eine virtuelle Maschine enthält, den Wartungsmodus und überprüfen Sie, ob die virtuelle Maschine zu einem alternativen Host migrieren kann.

Kapitel 6 Referenzdokumentation

In diesem Kapitel werden die folgenden Themen behandelt:

EMC Dokumentation **80**

Andere Dokumentationen **80**

EMC Dokumentation

Die folgenden Dokumente auf der EMC Online Support-Website bieten weitere und relevante Informationen. Der Zugriff auf diese Dokumente hängt von Ihren Anmeldedaten ab. Falls Sie auf ein Dokument nicht zugreifen können, wenden Sie sich an Ihren EMC Vertriebsmitarbeiter.

- *EMC XtremIO-Speicherarray – Benutzerhandbuch*
- *EMC XtremIO-Speicherarray – Benutzerhandbuch*
- *EMC XtremIO-Speicherarray – Handbuch zur Softwareinstallation und Upgrade*
- *EMC XtremIO-Speicherarray – Handbuch zur Hardwareinstallation und Upgrade*
- *EMC XtremIO-Speicherarray – Sicherheitskonfigurationsleitfaden*
- *EMC XtremIO-Speicherarray – Checkliste für Aufgaben vor der Installation*
- *EMC XtremIO-Speicherarray – Handbuch zur Vorbereitung des Aufstellorts*
- *Installationshandbuch für EMC VNX5400 Unified*
- *EMC VSI für VMware vSphere: Storage Viewer – Produktleitfaden*
- *EMC VSI für VMware vSphere: Unified Storage Management – Produktleitfaden*
- *VNX Installation Assistant for File/Unified – Arbeitsblatt*
- *VNX FAST Cache: ein detaillierter Überblick, White Paper*
- *Bereitstellen von virtuellen Microsoft Windows 8-Desktops: White Paper zur Anwendung von Best Practices*
- *Installations- und Administrationshandbuch für PowerPath/VE für VMware vSphere*
- *Installations- und Administrationshandbuch für EMC PowerPath Viewer*
- *EMC VNX Unified: Best Practices für Performance – Leitfaden zur Anwendung von Best Practices.*

Andere Dokumentationen

Die folgenden Dokumente auf der VMware-Website enthalten weitere und relevante Informationen:

- *Installations- und Einrichtungshandbuch für VMware vSphere*
- *VMware vSphere-Netzwerk*
- *Handbuch zur VMware vSphere-Ressourcenverwaltung*
- *Handbuch für VMware vSphere-Speicher*
- *vSphere-Administratorhandbuch für virtuelle Maschinen*
- *VMware vSphere-Handbuch für die Verwaltung virtueller Maschinen*
- *Handbuch für VMware vCenter Server- und Hostverwaltung*
- *Installieren und Verwalten von VMware vSphere Update Manager*

- *Vorbereiten der Update Manager-Datenbank*
- *Vorbereiten der vCenter Server-Datenbanken*
- *Management von Arbeitsspeicherressourcen in VMware vSphere 5.0*

Die folgenden Dokumente auf der Citrix-Website enthalten weitere und relevante Informationen:

- *Leitfaden zu XenApp 7.5 und XenDesktop 7.5*
- *Optimierungshandbuch für Windows 7 für die Desktopvirtualisierung.*
- *Optimierungshandbuch für Windows 8 und 8.1 für die Desktopvirtualisierung*

Die folgenden Dokumente auf der Microsoft-Website enthalten weitere und relevante Informationen:

- *Installieren von Windows Server 2012 R2*
- *SQL Server-Installation (SQL Server 2012)*

Appendix A Konfigurationsarbeitsblatt

In diesem Anhang wird das folgende Thema behandelt:

Arbeitsblatt für die Kundenkonfiguration 84

Arbeitsblatt für die Kundenkonfiguration

Bevor Sie die Lösung konfigurieren, müssen Sie einige kundenspezifische Konfigurationsangaben, z. B. IP-Adressen, Hostnamen usw., erfassen. In Tabelle 22 bis Tabelle 28 enthalten ein Arbeitsblatt, das Sie zur Aufzeichnung der Informationen verwenden können. Dieses Arbeitsblatt können Sie auch ausdrucken und dem Kunden als zukünftige Referenz überlassen.

Im Anhang zu diesem Dokument finden Sie eine eigenständige Kopie des Arbeitsblatts im Microsoft Office Word-Format. So zeigen Sie das Arbeitsblatt an und drucken es aus:

1. Öffnen Sie in Adobe Reader den Bereich **Attachments** wie folgt:
   - **Wählen Sie View › Show/Hide** › Navigation Panes › Attachments.
     oder
   - Klicken Sie auf das **Symbol Attachments**, wie in Abbildung 39 dargestellt.

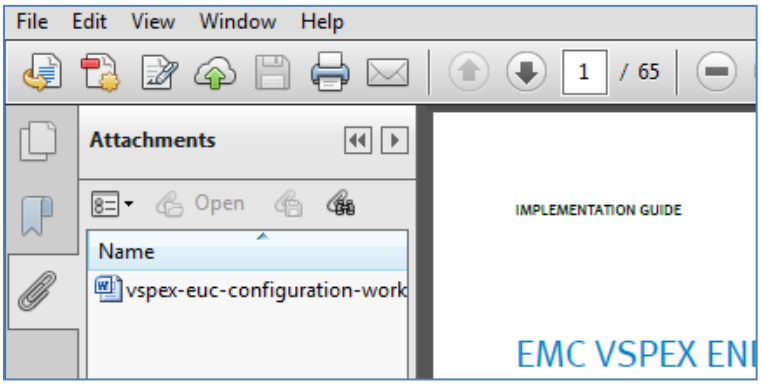

Abbildung 39. Öffnen von Anhängen in einer PDF-Datei

2. Doppelklicken Sie unter **Attachments** auf die angehängte Datei, um das Arbeitsblatt zu öffnen und auszudrucken.

Um die Kundenangaben zu bestätigen, überprüfen Sie das relevante Arraykonfigurationsarbeitsblatt: Arbeitsblatt *VNX Installationsassistent für File/Unified*.

Tabelle 22. Allgemeine Serverinformationen

Servername	Zweck	Primäre IP-Adresse
	Domain-Controller	
	Primäres DNS	
	Sekundäres DNS	
	DHCP	
	NTP	
	SMTP	
	SNMP	
	VMware vCenter-Konsole	

Servername	Zweck	Primäre IP-Adresse
	Citrix XenDesktop Desktop Delivery Controller-Server	
	Citrix Provisioning Services-Server	
	Microsoft SQL Server	

Tabelle 23. vSphere-Serverinformationen

Servername	Zweck	Primäre IP-Adresse	Private Netzadressen (Speicher)	IP-Adresse des VMkernel	vMotion-IP-Adresse
	vSphere-Host 1				
	vSphere-Host 2				
	...				

Tabelle 24. XtremIO-Arrayinformationen

Feld	Wert
Arrayname	
XMS-IP	
Speicher-Controller IPs	
Initiatorgruppennamen	
Datastore-Namen	

Tabelle 25. VNX-Arrayinformationen

Feld	Wert
Arrayname	
Administratorkonto	
Management-IP	
Name des Speicherpools	
Name des Datastore	

Tabelle 26. Informationen zur Netzwerkinfrastruktur

Name	Zweck	IP-Adresse	Subnetzmaske	Standard-Gateway
	Ethernet Switch 1			
	Ethernet Switch 2			
	...			

Tabelle 27. VLAN-Informationen

Name	Zweck des Netzwerks	VLAN ID	Zugelassene Subnetze
	Clientzugriffsnetzwerk		
	Speichernetzwerk		
	Managementnetzwerk		

Tabelle 28. Servicekonten

Konto	Zweck	Passwort (optional, angemessen gesichert)
	Windows Server-Administrator	
Root	vSphere-Root	
Root	XtremIO-Array-Root-Konto	
xmsupload	XtremIO-Array-xmsupload-Konto	
tech	XtremIO-Array-XMCLI-Tech-Konto	
Root	VNX-Array-Root	
	Arrayadministrator	
	VMware vCenter-Administrator	
	Citrix XenDesktop-Administrator	
	Citrix Provisioning Services-Administrator	
	SQL Server-Administrator	
	VMware vC Ops-Administrator	
	VMware vShield Manager-Administrator	